ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NETWORKS AND INFORMATION
INTEGRATION

OCT 2 7 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD AGENCIES

SUBJECT: Department of Defense (DoD) Command and Control (C2) Implementation Plan

The attached DoD C2 Implementation Plan delineates planning and execution responsibilities necessary to achieve the Department's C2 capability objectives and key actions codified in the DoD C2 Strategic Plan. It will be used to guide, synchronize, integrate, and coordinate C2 capability planning and implementation, and serve to inform Department governance and management processes. DoD components will use this DoD C2 Implementation Plan to collaboratively plan, coordinate and execute C2 capability related actions across the Department.

The DoD C2 Strategic Plan and this DoD C2 Implementation Plan satisfy requirements to develop and maintain a DoD C2 Roadmap under the provisions of DoD Directive O-5100.30 *DoD Command and Control*; and constitute the C2 Capability Portfolio Strategic Plan required by DoD Directive 7045.20 *Capability Portfolio Management.*

Cheryl J. Roby
Acting

Attachment:
As stated

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 OCT 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of Defense Command & Control Implementation Plan Version 1.0	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The Office of the Assistant Secretary of Defense for,Networks and Information Integration/DoD Chief Information Officer,6500 Defense Pentagon,Washington,DC,20301-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**81**	

DEPARTMENT OF DEFENSE
COMMAND & CONTROL IMPLEMENTATION PLAN

VERSION 1.0

1 October 2009

The Office of the Assistant Secretary of Defense for
Networks and Information Integration / DoD Chief Information Officer

Message from the Command and Control Capability Integration Board (C2CIB)

Tri-Chairs

Commanders must have the ability to command, control, and coordinate an integrated and interoperable force in rapidly changing conditions involving complex, distributed, simultaneous, or sequential operations. Command, control, and coordination within DoD and with external mission partners requires employment of integrated and interoperable capabilities that allow assigned forces to have visibility and easy access to information to effectively organize, understand, plan, decide, direct, and monitor the execution of operations in support of a commander's intent.

The initial DoD C2 Implementation Plan aims to expedite delivery of these capabilities in support of the Department's C2 objectives. The plan provides guidance to create unity of effort and incrementally advance toward Leader Centric, Net-Enabled C2 capabilities. It delineates execution responsibilities, provides an approach to synchronize and integrate implementation activities, and provides guidance to execute, monitor, and adjust those activities as the Department's needs and priorities change and new and more effective solutions are identified.

Execution of this plan requires effective governance and management to collaborate, coordinate, and implement activities across the Department of Defense enterprise, and in coordination with our mission partners. Governance and management activities, processes, and coordinating mechanisms must facilitate the integration of C2 implementation activities across the Department's Planning, Programming, Budgeting, and Execution, Defense Acquisition System, and Joint Capabilities Integration and Development System processes.

The C2CIB is committed to a comprehensive approach to define and implement a range of solutions that enable rapid development, fielding, and sustainment of resilient C2 organizational constructs, processes, concepts and technologies from national through tactical levels. The C2CIB will provide oversight to ensure the successful execution of this plan.

C.V. MAUNEY
Vice Admiral, USN
Deputy Commander
U.S. Strategic Command

Cheryl J. Roby
Acting, Assistant Secretary of Defense
Networks and Information Integration/
DoD Chief Information Officer

ROBERT S. HARWARD
Vice Admiral, U.S. Navy
Deputy Commander
U.S. Joint Forces Command

(This page is intentionally blank.)

CONTENTS

APPENDIXES

LIST OF FIGURES

LIST OF TABLES

(This page is intentionally blank.)

EXECUTIVE SUMMARY

The DoD C2 Implementation Plan delineates planning and execution responsibilities necessary to achieve the Department's C2 capability objectives and key actions as codified in the DoD C2 Strategic Plan. It also provides guidance for synchronizing C2 implementation activities across the Defense enterprise.

The DoD C2 Implementation Plan provides an approach for organizing C2 implementation activities and executing, monitoring, and adjusting those activities, as the Department's needs and priorities change and new and more effective solutions are identified across the C2 Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) spectrum. In addition, the DoD C2 Implementation Plan prescribes management activities, processes, and coordinating mechanisms that will facilitate the integration of C2 implementation activities across the Department's Planning, Programming, Budgeting, and Execution (PPBE) process; Defense Acquisition System (DAS); and Joint Capabilities Integration and Development System (JCIDS).

C2 implementation activities are organized into five implementation themes that were derived from an analysis of the DoD C2 Strategic Plan's objectives and key actions. These five implementation themes are:

- Achieving Leader-Centric C2
- Implementing Net-Enabled C2 Capabilities
- Implementing Interoperable C2 and Information Sharing among U.S. Forces and Multinational and Interagency Mission Partners
- Implementing Selected C2 Capabilities
  - Implementing Interoperable C2 of Joint Fires, Combat Identification (CID), and Friendly Force Tracking (FFT) Capabilities
  - Implementing Adaptive Planning and Execution
  - Implementing National and Nuclear Command Capabilities (Senior Leader C2)

- Implementing C2 Portfolio Management.

Specific implementation guidance consists of implementation activities for achieving the C2 objectives in the DoD C2 Strategic Plan. The execution of the implementation activities is phased across four timeframes where each implementation activity will have achieved its intended results by the end of 2010, 2012, 2014, or 2016.

1. INTRODUCTION

The DoD Command and Control Implementation Plan provides guidance and assigns responsibilities to achieve DoD command and control capability objectives directed by the DoD Command and Control Strategic Plan. This plan prescribes amplifying guidance and details an executable approach for the Department to effectively define, prioritize, acquire, govern, manage, and implement C2 capabilities consistent with the strategic direction contained in the DoD C2 Strategic Plan.[1] DoD C2 implementation planning is accomplished by the unified effort of the Office of the Secretary of Defense (OSD), the military departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the defense agencies, the DoD field activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD components") under the DoD C2 governance and management structure.[2] DoD C2 implementation planning is intended to meet the needs of senior leaders, commanders, and stakeholders across the range of DoD operations.

1.1 Purpose and Intended Use

The DoD C2 Implementation Plan identifies implementation activities and associated execution responsibilities necessary to achieve the Department's C2 capability objectives codified in the DoD C2 Strategic Plan. It provides the basis for DoD C2 governance and management assessments and recommendations to synchronize DoD component activities across the defense enterprise.

The DoD C2 Implementation Plan will be used to guide, synchronize, integrate, and coordinate planning and implementation activities at all levels. In particular, DoD components will use the DoD C2 Implementation Plan to collaboratively plan and

---

[1] The DoD C2 Strategic Plan, Version 1, dated December 18, 2008, coupled with the DoD C2 Implementation Plan satisfies the requirement of Department of Defense Directive (DoDD) O-5100.30, "DoD Command and Control," January 5, 2006, to develop and maintain a DoD C2 roadmap. Further, the DoD C2 Strategic Plan and Implementation Plan together constitute the C2 Capability Portfolio Strategic Plan required by DoDD 7045.20, "Capability Portfolio Management," September 25, 2008.

[2] Department of Defense Directive (DoDD) O-5100.30, "DoD Command and Control," January 5, 2006, assigns responsibilities for funding, managing, developing, acquiring, operating, maintaining, evaluating, and improving DoD C2 capabilities.

coordinate C2-related Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) actions across the Department. This plan forms the basis for developing recommendations and providing input for synchronizing and integrating C2 capabilities across the Planning, Programming, Budgeting, and Execution (PPBE) process; Defense Acquisition System (DAS); and Joint Capabilities Integration and Development System (JCIDS) and provides the means to help resolve issues that arise.

The DoD C2 Implementation Plan synchronizes C2 capability delivery and integration with capabilities from other portfolios. Additionally, it will:

- Provide an approach to managing operational risk during the transition from current to follow-on C2 capabilities
- Enable effective governance via existing decision support processes and governance authorities in accordance with Department priorities
- Support the development and execution of implementation activities to satisfy DoD C2 capability objectives—in terms of both leader-centric and net-enabled capability needs
- Be maintained by the C2 Capability Portfolio Manager (CPM) and updated every 2 years to address emerging C2 operational concepts, changing and reprioritized capability needs, and advancing C2 system-related technologies.

1.2 Applicability and Scope

This initial version of the DoD C2 Implementation Plan addresses the period encompassed by the Future Years Defense Program (FYDP) (2010-2015) and beyond the FYDP where appropriate guidance can be discerned. It also identifies near-term activities necessary to support fielding of C2 capabilities in response to urgent warfighting[3] needs.

Command and control capabilities must support the full range of operations and mission partners at the national, strategic, operational, and tactical levels. They must support all DoD operations including, but not limited to, defense and national leadership

[3] Warfighters and warfighting are commonly used terms to broadly describe all members of DoD when they are performing missions across the full range of DoD operations in war and peace. The full range of missions includes homeland defense and domestic civil support activities of the Department of Defense.

C2 (to include Nuclear C2 and Continuity of Government),[4] Homeland Defense-Defense Support of Civil Authorities (HD-DSCA) operations; Strategic Deterrence operations; Major Combat Operations (MCO); Irregular Warfare (IW) operations; Stability, Security, Transition and Reconstruction (SSTR) operations; Comprehensive National Cybersecurity Initiative (CNCI) activities; and Security Cooperation/Building Partnership Capacity support operations.[5]

While the intended scope of the DoD C2 Implementation Plan is quite broad, as stated above, this initial version of the plan focuses mainly on the specific key actions identified in the DoD C2 Strategic Plan.[6] Accordingly, many aspects of C2 are not specifically addressed in this initial version—including many aspects of military tactical C2. Subsequent updates to this plan are expected to address additional issues of importance as they become identified and prioritized by the DoD C2 community. Section 2.5 on assessing risk and Section 4 on management and governance identify ways to facilitate this reassessment and potential broadening of C2 implementation activities on a recurring basis.

1.3 Background

The DoD C2 Strategic Plan builds upon the Department's strategic guidance to provide an executable strategy to manage risk involved with current operations and to allocate resources for DoD C2 investments to enable the Department to maintain a dominant edge globally. That strategic direction and policy guidance was based in part on the comprehensive C2 task and gap analysis contained in the C2 Joint Capabilities Document (JCD).[7]

The overarching goal is to mature C2 capabilities, centered on leaders highly skilled in the art of command, and ensure they are net-enabled to the appropriate level.

---

[4] Intended capabilities are Defense and National Leadership Command Capabilities (DNLCC) as specified in DoDD S-5100.44, "Defense and National Leader Command Capability (DNLCC), July 9, 2008.

[5] It is noted that there is no authoritative source for this "operations taxonomy." This taxonomy is derived from multiple sources and is illustrative of DoD operations that DoD C2 capabilities support.

[6] The DoD C2 Strategic Plan key actions are listed in Table A1 in Appendix A.

[7] The C2 JCD was approved by the Joint Requirements Oversight Council (JROC) in Joint Requirements Oversight Council Memorandum (JROCM) 266-06, December 22, 2006. The updated JCD, version 2.0, was validated by the C2 Functional Capabilities Board (FCB) September 12, 2008.

Section 2.1 discusses this goal in greater detail. Achieving this goal requires unity of effort by DoD components in implementation planning and execution.

Implementation activities and assignment of responsibilities will synchronize the implementation planning of the DoD components. This synchronization will enable the unity of effort necessary for accelerating delivery of C2 capabilities efficiently across the defense enterprise.

2. CONTEXT FOR DOD C2 IMPLEMENTATION PLANNING AND EXECUTION

The DoD C2 Strategic Plan provides strategic direction and policy guidance to achieve unity of effort in attaining the Department's C2 capability objectives and facilitates transforming Department C2 capabilities through an integrated capability portfolio. The required capability objectives and implementing activities do not exist in a vacuum. As the Nation continues to confront adaptive and determined enemies, an understanding of the operational and technical context within which these capabilities exist, and planning occurs, is necessary to effectively execute implementing activities.

2.1 Operational Context for C2 Implementation Planning and Execution[8]

Today the Department faces many complex and dynamic missions that require the collective capabilities and efforts of many organizations. C2 capabilities are the linchpin of such missions. Commanders must have the ability to command, control, and coordinate an interdependent force including external mission partners in rapidly changing scenarios involving complex, distributed, simultaneous, or sequential operations.

This DoD C2 Implementation Plan strikes a balance between the art of war (human interface) and the science of war (technological solutions). The Implementation Plan emphasizes the inherently human aspects of C2, including, for example, the education and training of our Service members and the development of robust tactics, techniques, and procedures (TTPs), while clarifying the policies for technical advances and integration. The DoD C2 capability objectives, at their core, are about enabling leadership in complex, chaotic, and degraded information environments. C2 capabilities must be leader-centric and network-enabled to facilitate initiative and decision-making at the lowest appropriate level. In practice, this translates to a subordinate's ability to act without specific instructions, in accordance with commander's intent.

While advanced concepts and technologies associated with net-centricity may hold the promise of seemingly ubiquitous access to information, the Department's efforts in the C2 capability area will be guided by the principal maxim of command and control:

---

[8] The operational context for the DoD C2 Implementation Plan is derived from the DoD C2 Strategic Plan and the Capstone Concept for Joint Operations (CCJO) Version 3.0.

technology enables human interface and supports "command" and the decision maker, rather than forcing the decision maker to operate within the constraints of "control" technology. The DoD C2 capability development community will remain cognizant of this to ensure C2 technical solutions meet commanders' needs.

The foreseeable future promises to be an era of persistent conflict—a period of protracted confrontation among states, non-state entities, and individual actors increasingly willing to use violence to achieve their political ends. Future conflicts will continue to appear as hybrids of traditional and irregular warfare operations comprising diverse, dynamic, and simultaneous combinations of organizations, technologies, and techniques. One particularly important development in this environment is the increasing ability of other state and non-state actors to challenge the United States for influence. These emerging, advanced competitors pose significant regional challenges in the event of conflict. Non-state actors, often motivated by extremist ideologies, are emerging with some of the power of states, but lack the political discipline imposed by national sovereignty and accountability. Our DoD C2 capabilities must possess the agility and robustness to meet the operational demands of this persistent conflict environment.

2.2 Technical Context for C2 Capability Planning and Execution

Transformation of DoD C2 capabilities to an integrated, interdependent, leader-centric and net-enabled[9] capability portfolio is a goal of the Department. That transformation requires the establishment of a rich information-sharing environment with trusted information and functionality provided through assured services. Achieving this net-enabled vision will require a migration from the current system-based implementation construct towards a shared services-based environment. Data and services must be visible and accessible to eliminate information stovepipes and to enable operational agility.

The DoD C2 Strategic Plan characterizes the net-enabled, C2 systems framework of the future as shown in Figure 1. Depicted is a C2 systems enterprise within which C2 capabilities are provided as services from a user's perspective. Services that are accessible and provided within this enterprise, called a *service-oriented enterprise*

[9] In this context, the term "net-enabled" is used in its most generic sense—i.e., C2 operations facilitated through the use of information technology (IT) systems interconnected via a communication network or network of networks.

(SOE)[10] in this plan, include both the provision of data and C2 functionality. Service providers are depicted conceptually in the lower half of the diagram while service consumers are depicted in the upper half. Importantly, services are provided by a variety of sources including sources managed by the C2 CPM as well as other CPMs (e.g., Net-Centric, Battlespace Awareness, and Logistics). C2 platforms and facilities with reliable and robust access to a network will initially implement and migrate toward a SOE as conceptually depicted. However, a need will remain to retain some traditional point-to-point information exchange solutions until SOEs can be extended to disconnected, intermittent connection, or limited bandwidth (DIL) operational environments and can be shown to support the defined C2 capability needs of warfighting commanders at all levels.

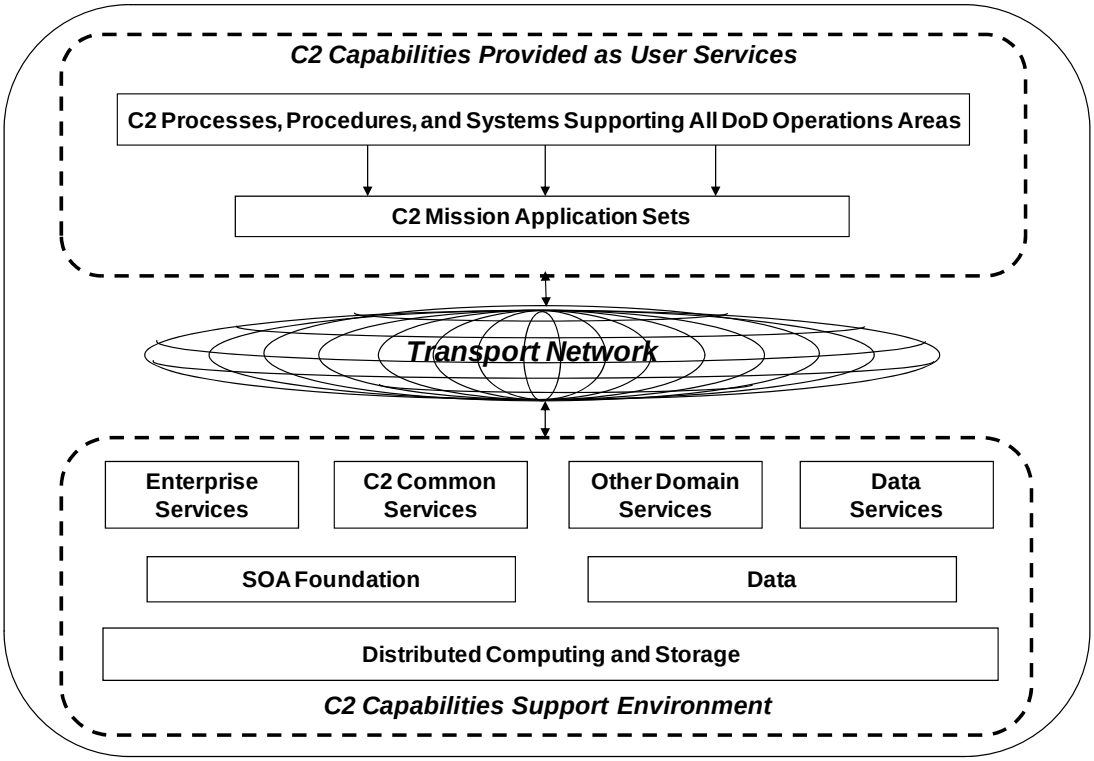

Figure 1. Conceptual C2 Systems Framework

[10] The term "service-oriented enterprise (SOE)" is intended to describe an enterprise that combines a services-focused way of doing business with the latest technology in an operational culture where participating entities are both *service providers* and *service consumers*. This term implies a broader approach to providing and using services than the term "service-oriented architecture (SOA)," which is used in Figure 1and implies the implementation of particular architectural or technical constructs. See Appendix B for definitions of both these terms.

Transitioning current C2 capabilities to a services-oriented enterprise has several important benefits and positions the Department to reduce unnecessary duplication of functions. Such an enterprise will provide C2 capabilities with support from common infrastructure services and access to data and services from other Joint Capability Areas (JCAs). The C2 capability development community must ensure no loss of capability to operational forces and senior leaders during migration from current to objective capabilities. Planning and executing the transition of C2 systems from the present-day client-server environment to a services-based, net-enabled enterprise is one of the major challenges facing the Department today.

2.3 Approach to DoD C2 Capabilities Implementation Planning and Execution

Achieving DoD's C2 capability objectives requires collaborative and coordinated implementation planning and execution activities by all DoD components, interagency partners, and allies. Achieving these objectives also requires a comprehensive and consistent approach for defining a range of DOTMLPF solutions that enable rapid development, fielding, and sustainment of transformational C2 organizational constructs, processes, supporting concepts, and technologies from the national to the tactical level. All components are expected to actively participate in formulating and executing this approach.

This DoD C2 Implementation Plan describes an approach to planning and execution activities that emphasizes incremental delivery of improved capabilities over time. Implementation planning is a C2 CPM-facilitated activity that involves identifying and prioritizing increments of C2 capabilities that are operationally meaningful, technically feasible, programmatically achievable, and fiscally affordable. Execution involves activities led by combatant commands, Services, and agencies (C/S/As) that are facilitated and integrated across the full DOTMLPF spectrum by the C2 CPM to enable incremental improvements. Implementation planning and execution activities must be synchronized, managed, and governed effectively to ensure attainment of the Department's C2 capability objectives.

Figure 2 depicts a conceptual approach for sequencing activities to enable incremental improvements in C2 over time. A fundamental underpinning of this approach is a C2 capability delivery increment (CDI) construct that identifies measurable time-phased improvements in C2 capabilities through a JCA framework. The CDIs

notionally depicted as four increasingly improved capability states are consistent with the draft CDIs currently under development. The DoD C2 Strategic Plan also requires the identification of appropriate metrics to facilitate monitoring CDI-derived implementation planning and execution actions towards attainment of the Department's C2 capability objectives.

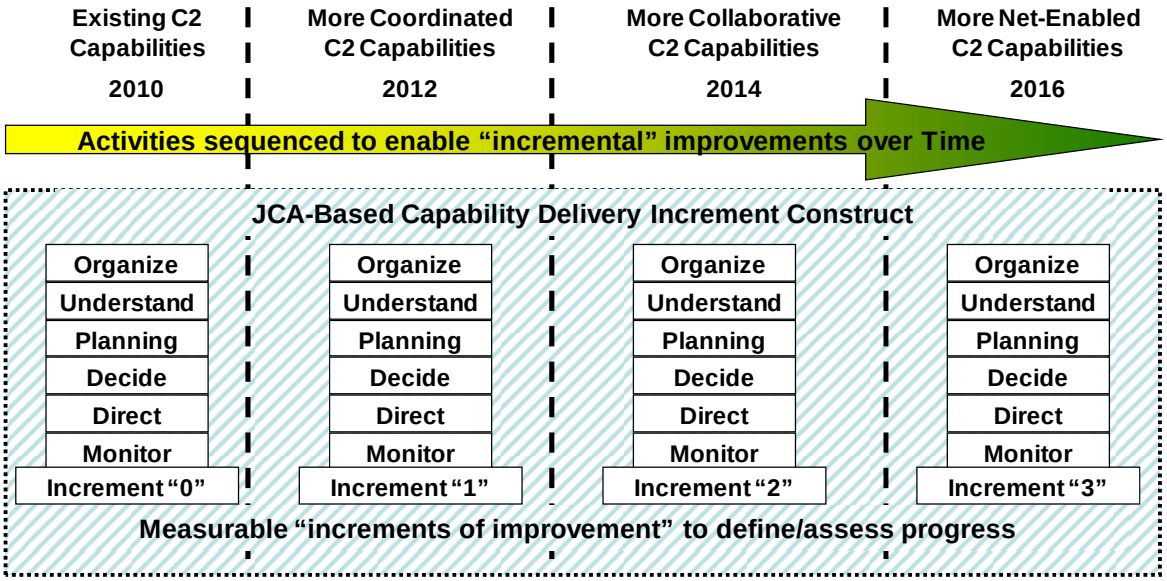

Figure 2. Conceptual Approach to Implementation Planning and Execution

The approach requires sufficient understanding of current capabilities defined through analysis of fielded systems and existing developmental programs and informed by the C2 Joint Capabilities Document (JCD), combatant command Integrated Priority Lists (IPLs), and related capability-based analyses. It is framed by the DoD C2 Strategic Plan's objectives and key actions with input from C2 community-wide planning analyses. This approach provides a means to identify, sequence, synchronize, and integrate planning and execution activities to attain the capability states shown notionally in Figure 2 across the DOTMLPF spectrum, consistent with Department priorities.

A number of related activities bound and affect the Department's ability to achieve measurable improvements across all increments of DoD C2 capabilities. These include planning and execution actions that (1) implement the Department's Net-Centric

Data and Services Strategies,[11] (2) more effectively balance DOTMLPF analysis and enhanced synchronization, (3) more effectively and efficiently govern and manage the C2 Portfolio to support warfighters across the range of military operations at all levels and, (4) provide the means for process improvements in both C2 functions as well as the integration of the Department's decision-making processes. These activities affect all capability increments and require evolutionary application to enable effective migration from current to objective capability states.

Two supporting analytical activities are taking place whose purpose is to directly influence C2 capability development and implementation planning and mature the approach in Figure 2: the development of CDIs and the FY08-09 Optimum Capability Mix Study (OCMS).[12] The CDI and OCMS efforts are being executed concurrently with the development of this initial DoD C2 Implementation Plan—and several important artifacts of that work (e.g., specific timeframes and characterizations of CDI-related capability descriptors) are reflected in Figure 2. While preliminary results of the CDI and OCMS efforts have informed this version of DoD's C2 Implementation Plan, further harmonization of these analytical and planning activities with the DoD C2 Strategic Plan's objectives and key actions and the DoD C2 Implementation Plan's implementation activities is still required.

The C2 CPM will continue to mature the C2 CDIs in parallel with ongoing DoD C2 implementation planning with the purpose of further defining CDIs and associated metrics that can enable effective management of C2 implementation activities as required by the DoD C2 Strategic Plan. Once vetted and approved, the Implementation Plan will adopt the approved CDIs as the primary source of planning and delivery of C2 capabilities to the Department consistent with portfolio management and Services' Title 10 authorities. The objective for completing this CDI/DoD C2 Implementation Plan harmonization is 6 months after approval of the DoD C2 Implementation Plan.

---

[11] DoD Chief Information Officer Memorandum, "DoD Net-Centric Data Strategy," May 9, 2003; Department of Defense "Net-Centric Services Strategy," DoD CIO, May 4, 2007; and DoDD 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

[12] The FY08-09 OCMS is being conducted by U.S. Joint Forces Command (USJFCOM) in response to direction from OSD to estimate the optimum mix of C2 capabilities needed for strategic, operational, and tactical military operations in the 2014-2016 timeframe.

2.4 Approach to Organizing Implementation Planning and Execution Activities

The approach for C2 implementation planning and execution described in this plan uses an organizing construct for articulating, sequencing, and synchronizing discrete implementation activities and also assigning responsibilities and timelines for execution. This organizing construct, at maturity, provides the means to monitor those activities and make timely adjustments to C2 implementation planning and execution as warfighters' needs and Department priorities change and/or as new and more effective solutions are identified. As emphasized in the DoD C2 Strategic Plan, the Department must effectively integrate all C2 capability-related DOTMLPF activities—specifically within the context of the JCIDS, DAS, and PPBE processes.[13] The organizing construct for this Implementation Plan consists of two complementary sets of activities:

- Implementation activities related to achieving DoD's C2 objectives and associated key actions—as articulated in the DoD C2 Strategic Plan
- Management activities, processes, and coordinating mechanisms that facilitate the integration of C2 implementation across the DOTMLPF spectrum.

This DoD C2 Implementation Plan organizes these two sets of activities into themes, which is the construct for providing implementation guidance in Sections 3 and 4. Guidance is provided in the form of tables that list specific implementation activities, assignment of execution responsibilities, and timeframes for completion. The execution of the implementation activities is phased across four timeframes where each implementation activity will achieve its intended results by the end of 2010, 2012, 2014, or 2016.

2.4.1 Approach to Implementation Themes

Specific implementation themes contained in this initial DoD C2 Implementation Plan are tied to objectives and key actions identified in the DoD C2 Strategic Plan. The key actions were analyzed to identify implementation activities that, if executed successfully, would accomplish the key action. Implementation activities were then organized into implementation themes to facilitate collaborative execution and unity of

[13] See current Department directives and issuances regarding the Joint Capabilities Integration and Development System (JCIDS), the Defense Acquisition System (DAS), and the Planning, Programming, Budgeting, and Execution (PPBE) process.

effort in achieving DoD C2 Strategic Plan objectives.[14] This analysis resulted in the identification of five implementation themes—four that relate directly to enhancing C2 capabilities and one that relates to management of C2 implementation activities. These five implementation themes are:

- *Achieving Leader-Centric C2*: implementation activities that address the enhancement of all leader-centric DOTMLPF aspects of C2
- *Implementing Net-Enabled C2 Capabilities*:[15] implementation activities that address the incremental evolution of services-based C2 systems and supporting infrastructure environments—and the migration of legacy systems to those environments
- *Implementing Interoperable C2 and Information Sharing among U.S. Forces and Multinational and Interagency Mission Partners*: implementation activities that leverage net-enabled capabilities to enhance operational interoperability and information sharing
- *Implementing Selected C2 Capabilities*: implementation activities that address specific capability needs that received special emphasis in the DoD C2 Strategic Plan. Three such capability areas are:
  - Implementing Interoperable C2 of Joint Fires, combat identification (CID), and friendly force tracking (FFT) Capabilities
  - Implementing Adaptive Planning and Execution
  - Implementing National and Nuclear Command Capability (Senior Leader C2)
- *Implementing C2 Capability Portfolio Management*: implementation activities that can facilitate planning, analysis, management, and integration of all implementation activities.

---

[14] The analytic process used to derive implementation themes from the Strategic Plan key actions is described in Appendix A.

[15] As stated in paragraph 2.2, the term "net-enabled" is used here in its most generic sense—i.e., C2 operations facilitated through the use of information technology (IT) systems interconnected via a communication network or network of networks. In terms of technical implementation, it is understood that the term "net-enabled" often has a much more specific meaning—i.e., the ability of an application, system, or function to be accessed and used via an IP-based network (vice a local client); or to characterize an incremental step in system development such as that from client-server-based capability to net-centric or SOA-based capability.

2.4.2 Approach to Governance and Management of Implementation Activities

DoD C2 planning and execution involves a range of activities that are formally assigned through the DoD C2 governance and management construct.[16] The DoD C2 Strategic Plan identifies the need for a common framework within which to conduct, manage, and synchronize all C2-related JCIDS, PPBE, and DAS activities.[17] That framework is intended to incorporate CDI metrics to enable the Department to monitor progress in executing this Implementation Plan.

This Implementation Plan describes and codifies an integrating framework as the basis for the execution, management, and oversight of C2 implementation planning and execution activities—to include cross-portfolio coordination and synchronization. Section 4 provides guidance for implementing C2 portfolio-related governance and management activities.

2.5 Approach to Managing Risk

The DoD C2 Strategic Plan emphasizes the need to address both operational and programmatic risk in C2 implementation planning and execution. Operational risk assessments are made by combatant commanders and Services. Programmatic risk is focused on capability development, return on investment, and program executability. The JCIDS process is initiated through the execution of a capabilities-based assessment (CBA). CBAs help identify gaps in the abilities of a C/S/A to execute assigned missions and assess associated risk(s).

Implementation activity offices of primary responsibility (OPRs) will consider both the operational risk assessments and the programmatic risks. In these deliberations, OPRs will weigh willingness to accept operational and/or programmatic risk; identify and consider interdependencies, which could positively or negatively affect success in realizing the implementation activity objective; and ensure that implementation decisions are openly vetted with capability stakeholders.

---

[16] DoDD O-5100.30, "DoD Command and Control," January 5, 2006; CJCSI 3265.01, "Command and Control Governance and Management," September 22, 2008; and DoDD 7045.20, "Capability Portfolio Management," September 25, 2008, all pertain.

[17] This subject is discussed in paragraph 3.1 of the DoD C2 Strategic Plan.

The C2 CPM considers risk during all analysis and deliberations. It will seek the advice and endorsement of the C2 Senior Warfighter Forum (SWarF) on that analysis and major portfolio decisions in order to ensure that the warfighter's view of operational risk is heard, understood, and addressed appropriately. The C2 SWarF will provide feedback to the C2 CPM.

Formal risk assessments are informed by the Department's strategic guidance, current operational demands, and fiscal realities. Deliberations dealing with transitions from existing to new C2 capabilities, or reprioritization of capability needs, will emphasize a risk-based approach weighted toward warfighter considerations. At a minimum, implementation planning activities and capability deliveries must ensure that while transitioning to new desired capabilities there is no reduction in current capability relevant to operations. This imperative is commonly referred to as the "Do no harm" strategy.

3. C2 CAPABILITY IMPLEMENTATION GUIDANCE

This section prescribes guidance for executing and synchronizing implementation activities to enable incremental improvements in C2 capabilities. The guidance is organized according to implementation themes discussed in the previous section and provides implementation activities, timeframe, and lead and supporting organizations in a series of tables and associated text that describe activities necessary to accomplish the key actions identified in the DoD C2 Strategic Plan.

3.1 Achieving Leader-Centric C2

C2 is first and foremost a human endeavor. DoD C2 must be leader-centric and net-enabled to facilitate initiative and decision-making at the lowest level possible. While materiel solutions, processes, and engineering can enable decision making, command and control is not synonymous with network operations or employment of advanced technology. Rather, it maintains the flexibility to exploit both. Consequently, commanders must be skillful at crafting their commander's intent, enabling junior leaders to exercise initiative and take advantage of fleeting opportunities in the heat of battle, vice centralizing decision-making at high levels. This is particularly important in fast-paced conventional force-on-force warfare and during highly dynamic and decentralized operations that characterize hybrid and irregular warfare. The phrase "leader-centric and net-enabled" refers to a balance between the art of war (human interface) and the science of war (technological solutions). A net-enabled force maintains the flexibility to exploit advantages of network operations and employment of advanced technology without hindering the initiative of skilled and ready forces. In an operational context, this translates to a subordinate's ability to act without specific instructions per commander's intent.

While C2 is a leader-centric activity, materiel programs and systems are also significant from a total capabilities perspective. To compensate for increased risks, DoD must ensure our C2 systems, and their associated networks, are resistant to attack and are robust enough to reconstitute quickly if a successful attack takes place. Throughout these challenges, our leaders must still be able to execute missions using decentralized decision-making consistent with their commander's intent in degraded information environments, so leaders and their subordinate forces are not paralyzed when network degradation occurs.

The key actions from the DoD C2 Strategic Plan that relate directly to the human elements of C2 (key actions 1.5 and 5.1) are addressed below.

3.1.1 C2 Leadership Training and Education

Many valuable lessons can be gleaned from American leadership experiences in the Philippines, Vietnam, Central America, Somalia, and now Iraq and Afghanistan—lessons that emphasize the need for capabilities to conduct operations in complex, chaotic, and hostile environments. Key among these lessons is for leaders to understand (a tier II C2 JCA) the culture, beliefs, values, and expectations of the relevant population and to work closely with and within that population. This is fundamental to success. Similar lessons come from DoD civil support experience in 9/11, Hurricane Katrina, and the Indonesian tsunami. Leader training and education is critical to building such understanding and enabling leaders and their staffs to operate more effectively in a hybrid operating environment—that is, an environment that includes both traditional and irregular warfare operations. Joint training, professional military education, and cultural awareness are key enablers to developing warfighters for future operations and leaders with flexible and creative problem-solving skills. Leaders, down to the lowest levels, must be capable of acting on their own authority based on an understanding of the situation and an appreciation for the implications of their actions. In practice, this translates to a subordinate's ability to act without detailed instructions, in accordance with commander's intent. In order for that to happen, the commander must skillfully develop a sound, well-articulated intent grounded in realistic assessments of the operating environment and including considerations of mission partners.

Improvements in C2 training are particularly needed at the lower tactical levels of war. In humanitarian and consequence management environments, both commanders' intent and subordinate commander initiative are often bounded by the mission request/mission tasking nature of many of these operations in support of civil authorities. Furthermore, general purpose forces need to operate effectively in complex warfare environments that place a premium on effective small unit operations. Several initiatives are underway in this area that should be supported. These include the Future Immersive Training Environment (FITE) Joint Capability Technology Demonstration (JCTD), which has the desired end state of transitioning specific immersive training technologies to the Services. The FITE JCTD provides enhanced Service training technology capabilities by providing a realistic, full-sensory training environment. In particular, it

will hone small unit trainees' decision-making skills in a complex, fast-paced training situation with legal, moral, and ethical issues. The FITE JCTD is the first step in the larger National Program for Small Unit Excellence (NPSUE) that will bring national-level attention to the problem of recruiting, educating, and training individuals, leaders, and small units to deal with the threats of today and tomorrow. NPSUE will enlist the help of social scientists, psychologists, leader development experts, small unit leaders, and first responders. A series of forums hosted in 2010 will address performance under stress in small unit scenarios and culminate in a long-range plan to improve small unit performance.

Finally, understanding collaborative processes and tools is key to the success of future leaders and decision makers. Effective operations in complex, chaotic, or hostile environments require a solid training and educational foundation. In accordance with the DoD Information Sharing Implementation Plan, Tasks 2.3 and 4.1, a critical facet of this foundation must be training, education, and exercise of information sharing roles.[18] DoD must invest in the education and training of all leaders commensurate with attention to technical programs. For the domestic environment, concepts such as rules of force versus rules of engagement and how to execute operations by Essential Support Functions (ESF) need to be taught, trained, and exercised.

Table 1 lists the C2 training and education implementation activities needed to accomplish key actions from the DoD C2 Strategic Plan.

[18] DoD Information Sharing Implementation Plan, April 2009, Task 2.3, "Educate and train personnel on their roles in information sharing," and Task 4.1, "Develop an approach that ensures information sharing activities (policies, procedures, and technologies) are integrated into appropriate joint experiments, demonstrations, and exercises."

Table 1. C2 Training and Education Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Conduct joint and Service training review at all levels of command to identify joint C2 gaps and shortfalls. Emphasis should be placed on the capability to operate effectively in complex, chaotic, and hostile environments.	5.1		X			Joint Staff	Services USJFCOM
Incorporate approved recommendations of Joint and Service Training review into JPME and Service schools increasing emphasis on joint leadership training and education.	5.1			X		Joint Staff	Services USJFCOM
Provide reinforced unit-level training capability with integrated, interoperable, and immersive elements.	5.1	X				USJFCOM	Services USD(AT&L)
Implement a comprehensive policy for establishing and operating collaborative information environments[19] that accommodate coalition and non-traditional partners.	1.4, 2.2, 2.3, 3.1, 3.2			X		OASD(NII)/DoD CIO	USD(P)
Develop leadership training and TTPs for utilization of information management constructs in collaborative information environments.[20]	1.4, 3.1, 3.2		X			USJFCOM	Services

[19] See Appendix B for definition of collaborative information environment (CIE).

[20] See policies contained in DoDD 8100.02, "Multinational Information Sharing (MNIS) Implementation"; DoDD 8500.01E, "Information Assurance"; and DoDD 8521E, "DoD Biometrics."

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Create standardized TTPs for employment of enterprise-level collaborative capabilities.	1.4, 3.1, 3.2	X				USJFCOM	Services
Develop an approach that ensures information sharing activities (policies, procedures, and technologies) are integrated into appropriate joint experiments, demonstrations, and exercises.	1.4, 3.1, 3.2, 5.1		X			USJFCOM	USD(AT&L) Combatant commands Secretaries of the Military Departments

3.1.2 JTF Headquarters Command and Control

Combatant commanders' ability to sustain the readiness of Service operational headquarters (HQ) designated as JTF Capable HQ is constrained by a combination of manpower, equipment, and training issues, as well as shortfalls in readiness reporting guidance and tools/systems. Similarly, a JTF commanders' ability to coordinate military operations with non-DoD organizations (including coalition and allied partners, other government agencies, international organizations, and non-governmental organizations) is constrained by technical and policy-based information-sharing issues and a lack of understanding and knowledge of non-DoD organizations. As a result of QDR 2006, the Department undertook a task to enable existing Service operational headquarters to perform as scalable JTF Capable HQ. Inherent to the task is the need to organize, man, train, and equip selected Service operational headquarters to make them JTF Capable, available and ready to command and control designated joint force missions. Toward that end, a JTF Headquarters handbook is under development, intended to provide considerations and practices from which combatant commanders and the Services can begin a process to continually improve readiness of operational-level command and control headquarters.

Similarly, DoD has created Joint Force Headquarters-State (JFHQ-State) and JTF command elements in 54 states and territories. It has also implemented a Joint CONUS Communication Support Environment (JCCSE) concept to enable interoperability and information sharing with domestic responders. USNORTHCOM provides formal JTF-

State command element training and conducts quarterly exercises. The JFHQ-State and JTF-State command elements rely on government off-the-shelf (GOTS) IT systems and integrated commercial deployable communications systems. In 2008 the JROC advocated that these capabilities migrate into Service programs of record.

Table 2 lists implementing activities for the continued fielding of Service HQ designated as JTF Capable HQs.

Table 2. Joint C2 JTF Capable HQ Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Complete the JTF HQ handbook providing procedures for sustaining readiness of JTF Capable HQ.	1.5	X				USJFCOM	Combatant commands Services
Analyze training, equipment & technology, and readiness reporting issues impacting readiness of Service HQ designated as JTF Capable HQ. Include consideration of impact on mission partners. Take appropriate action via DOTMLPF Change Recommendations and recommended policy changes.	1.5	X				USJFCOM	Combatant commands Services USSOCOM
Establish a Global Force Management (GFM) process, business rules, and procedures for prioritization of combatant commander JTF HQ requirements relative to other operational requirements.	1.5		X			USJFCOM	Joint Staff

3.2 Implementing Net-Enabled C2 Capabilities[21]

In order to facilitate *net-enabled* military operations (i.e., operations characterized by shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization), the Department has advocated and supported initiatives to implement *net-centric* command and control; communications; and intelligence, surveillance, and reconnaissance (ISR), along with associated processing, exploitation, and dissemination (PED) capabilities. Such capabilities are needed to support worldwide and domestic C2 and situational awareness (SA) operational requirements and are envisioned to be achieved through either the transformation or replacement of current capabilities. Given the overall goal to achieve these capabilities as soon as possible and at an affordable cost, the Department must continuously assess alternative system and network implementation strategies. Some operational capabilities can be relatively easily evolved through enhancements to current systems (e.g., providing access to web-based information and services). Others will require significant reengineering of both operational processes and enabling IT systems. The most prudent and cost-effective strategy will likely include a combination of legacy system transformations and development of new systems based on net-centric architectures and technologies from the beginning.

This section addresses the *Implementation of Net-Enabled C2 Capabilities* theme—as articulated in Sections 2.2 and 2.4 of this DoD C2 Implementation Plan. Additionally, as a result of the analysis of DoD C2 Strategic Plan key actions, this section identifies a number of specific C2 implementation activities. Implementation of many enabling capabilities is the responsibility of the Net-Centric (NC) CPM and the DoD components. Accordingly, close coordination between the C2 CPM and the NC CPM is essential to achieving the Department's operational objectives. The Command and Control Capability Integration Board (C2 CIB) provides oversight and direction for the C2 and NC CPMs and is key to ensuring seamless coordination between them. The requirement for cross-CPM coordination of implementation activities under the *Net-Enabled C2 Capabilities* theme will, in general, be the rule rather than the exception.

---

[21] Given the technical nature of the discussion in this section, the term "net-centric" is used to characterize the objective state of "net-enabled" C2 capabilities and to address compliance with current DoD issuances regarding the implementation of net-centricity in the DoD.

The discussion of net-enabled C2 and guidance for executing related implementation activities are organized here into the following four sub-topics:

- Net-Centric Data and Services Implementation
- Migrating to a Service-Oriented Enterprise (SOE)
- Assured Information Exchange Services
- C2 in Tactical and Austere Operating Conditions.

3.2.1 Net-Centric Data and Services Implementation

Implementation of the Department's Net-Centric Data Strategy (NCDS) and Net-Centric Services Strategy (NCSS)[22] is essential to providing the warfighter with a responsive and interoperable C2 systems environment. Operators at all levels of command must be enabled to discover, access, understand, receive, transmit, publish, use, and manipulate data through resilient and robust C2 and network services.

The Department initiated several activities in 2008 to help detail an approach for implementing the NCDS and NCSS in the C2 domain. As a result, the DoD CIO issued *Interim Implementation Guidance for the Net-Centric Data Strategy for the C2 Capability Portfolio* in a March 11, 2009 memorandum. This interim guidance identified a *C2 Information Sharing Framework (C2ISF)* and a *C2 Core* (both described below) as critical components for implementing the NCDS and NCSS. The DoD CIO's guidance memorandum also directed further development of the C2ISF and C2 Core concepts, specifications, and the associated approaches for NCDS and NCSS implementation in the C2 domain in a follow-on program of work to be accomplished (See Table 3).

The C2ISF is a services-based organizing construct that consists of: (1) design-time artifacts, standards and transformation algorithms that contribute to structurally and semantically compatible data sharing solutions based on the Universal Core (Ucore) (defined below in connection with the C2 Core), the C2 Core, and other related initiatives; and (2) physical run-time infrastructure capabilities that exploit DoD enterprise, community and local infrastructures to include service and metadata registries, content catalogs, access control arrangements, mediators, crawlers, and tagging engines.

[22] Department guidance in these areas is provided in DoD Chief Information Officer Memorandum, "DoD Net-Centric Data Strategy," May 9, 2003; Department of Defense "Net-Centric Services Strategy," DoD CIO, May 4, 2007; and DoDD 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

C2ISF-related services will be designed, federated, and otherwise adapted to enable information sharing in a SOE environment. Service and content discovery, instrumentation to monitor status and provide metrics collection, anecdotal user feedback arrangements, and development/testing tool kits are some of the capabilities that will be provided within the C2ISF. The C2ISF is expected to mature over time as an organizing construct to help facilitate adaptive interoperability among components represented in the lower half of Figure 1 in both design and run-time environments.

An important enabler that can mitigate the information-sharing challenges posed to the C2 Capability Portfolio is the UCore, an interagency information exchange specification and implementation profile.[23] This published "emerging standard" offers developers and program managers a framework for commonly used data concepts of "who, what, when, and where." The UCore serves as a starting point for data level integration augmented by extensions to support domain and/or mission specific data exchanges. For the C2 capability portfolio, data level integration will be achieved through employment of the UCore extended by the C2 Core and COI or mission-specific extensions.

The C2 Core is a set of reusable metadata artifacts based upon rules to create C2-specific UCore extensions and information exchange specifications within a framework that supports C2 capabilities through the implementation, monitoring, and measurement of interoperable and assured information exchanges. The C2 Core, when developed, tested, and published by the C2 CPM, will support information exchanges within the C2 functional area and will address Task 9.2 in the DoD Information Sharing Implementation Plan.[24] The C2 Core will include extension rules consistent with UCore guidelines, naming and design rules, and a configuration management process to manage data artifacts created to enable new C2 capabilities. It will include the Joint C2 Conceptual Model and Vocabulary, which is a set of re-usable components covering the most common type of information exchanged within C2. The C2 service description

---

[23] See "DoD Defense Information Enterprise Architecture," Version 1.0, April 11, 2008; OASD (NII/DoD CIO)/Associate Director of National Intelligence CIO Memo, "Department of Defense and Intelligence Community (IC) Initial Release of Universal Core (UCore)," April 17, 2008; and DoD Deputy CIO Memo, "Universal Core (UCore) Guidance in Support of Enhanced Information Sharing," July 13, 2009.

[24] *DoD Information Sharing Implementation Plan*, April 2009, Task 9.2: "Continue to develop and improve data standards for the exchange of basic information elements across the DoD enterprise."

templates (as additional components of the C2ISF) will enable the design of web services and other C2 services required to support net-enabled C2 capabilities. The extension rules, re-usable components, and C2 service description templates are critical for programs and COIs to generate mission-specific metadata that conform to the UCore and C2 Core and support the C2ISF.

To help assess data and service implementation in support of C2 capabilities, Information Support Plans (ISPs) will be used to document program implementation plans and progress in data and service visibility, accessibility, and understandability. Metrics are an important part of the process and should be collected in an automated fashion, as appropriate, and used to assess implementation gaps in C2 capabilities and shortfalls in enterprise services. The C2 CPM will inventory existing metrics and use the appropriate metric for measuring C2 capabilities across the C2 domain. By measuring implementation progress, DoD Principal Staff Assistants (PSAs), the C2 CPM, and DoD components can assess the adequacy of data exposure, data services, and coordination of data needs to ensure proper positioning of data sources to support C2 capabilities.

Table 3 lists activities associated with the implementation of the Department's Net-Centric Data and Services Strategy. Accomplishment of the implementation activities in Table 3 constitutes the main effort for laying the foundation for migration to a service oriented enterprise.

Table 3. Net-Centric Data and Services Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Develop the C2 Core artifacts in compliance with the UCore and other registered meta-data. Register the C2 Core artifacts in DoD Metadata Registry (MDR).	3.4	X				USJFCOM OASD(NII)/ DoD CIO	Services DISA
Conduct C2 Core testing to verify, validate, and mature products and processes to include the configuration management process.	3.4	X	X			USJFCOM OASD(NII)/ DoD CIO	Services DISA

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Develop C2 Service Description Templates for C2 service providers at all echelons of command and further define the C2ISF and its use in evolving a C2 SOE.	3.4	X				OASD(NII)/ DoD CIO	USJFCOM
Identify authoritative data sources supporting C2 capabilities (C2 ADS).	3.4	X				USJFCOM DoD components	OASD(NII)/ DoD CIO
Coordinate ADS exposure schedules.	3.4	X	X			USJFCOM	DoD components
Develop methods to measure, monitor, and report utilization, value, and consumption of data and services, progress in C2 data and service implementation, and service and data exposure status.	3.4		X			OASD(NII)/ DoD CIO	Services USJFCOM DISA

3.2.2 Migrating to a Service-Oriented Enterprise (SOE)

Many of today's C2 systems and applications have stand-alone or limited data exchange capabilities that make interoperability complex and the introduction of new capabilities time-consuming and costly. Evolving to a net-enabled environment is intended to reduce functional redundancy, improve interoperability, and accelerate the integration and deployment of C2 enhancements to meet the operational needs of senior leaders, commanders, and forces. C2 programs and systems based on service-oriented constructs will enable the sharing and reuse of existing services and the ability to develop ad hoc functionality much more readily.

Migration to a service-oriented enterprise means moving to an environment of integrated processes and a shared set of composable C2 services. An important objective of migration to a SOE is to exploit broad access to net-centric data and services. However, notwithstanding the committed transition to service-oriented design and integration, the need exists to continue to retain some traditional point-to-point

information exchange solutions until a SOE solution can be shown to accommodate a variety of modes of operation [disconnected, intermittent connection, or limited bandwidth (DIL)] and provide the defined capability needs of warfighting commanders at all levels of C2. Another area with migration challenges is DSCA where some information-sharing capabilities used by DoD are not in applicable DoD migration plans or DoD programs of record (e.g., Homeland Security Information Network [HSIN]).

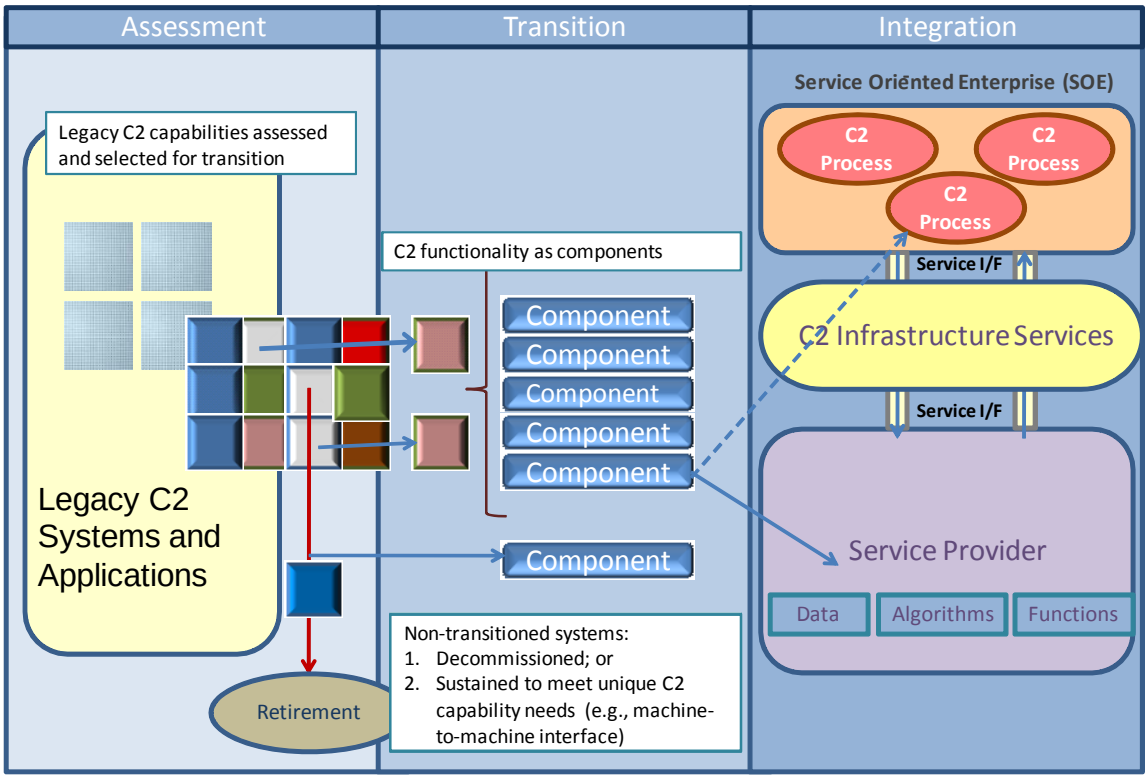

Figure 3. C2 System Migration Planning

Figure 3 depicts a conceptual approach for planning the transformation or migration of current system capabilities to the SOE shown in Figure 1. It is imperative that, in planning how best to evolve C2 capabilities to a SOE within fiscal constraints, the maintenance of current capability (especially in terms of performance, information assurance, and mission support) be given first priority. This is accomplished by measuring and assessing the current functionality and capability provided to the warfighter to establish the "As Is" baseline. (Refer to the left side of Figure 3). This involves the use of both qualitative and quantitative metrics to determine the level of

performance and functionality provided to and consumed by the C2 user and mission processes. Transition plans (the center portion of Figure 3) need to identify actions to mitigate risk and provide uninterrupted C2 capability throughout the transitioning phase. Measuring functionality and performance as C2 components are integrated into the "To Be" or objective SOE confirms that the provided capability is at or above the level of the current systems.

To accelerate the transition to an environment of integrated data and C2 services, Services and agencies are aggressively moving ahead to leverage Service- and enterprise-provided data and functional services such as Net-Centric Enterprise Services (NCES), Consolidated Afloat Network and Enterprise Services (CANES), and Marine Corps Enterprise Information Technology Services (MCEITS). Without the development and implementation of common C2 reference architectures, service specifications, and information-sharing frameworks, Service initiatives can vary in their approach to service-oriented design and potentially put joint interoperability at risk.

Changes necessary for an enterprise-wide adoption of service-oriented design constructs can only be achieved by putting the right policies and processes in place to bridge the enterprise architecture (EA) requirements with implementation strategy. Governance is an essential element of a services-oriented enterprise—it creates, communicates, and enforces policies, defines roles and responsibilities, and aligns IT investments with goals. Establishing and tracking key performance indicators to measure the effectiveness of governance is essential. Examples of measures and metrics include the number of applications using shared services, compliance with reference architectures, and adoption of enterprise standards.

An important enabler in this process is the use of rationalization[25] to assess current ("As Is") systems in order to identify candidate applications for decommissioning and those for migration as "best of breed" providers of C2 services. This is done as part of assessment and transitioning activities as shown in Figure 3. This method uses cost,

[25] In this context, rationalization means a systematic method for analyzing the state of systems, applications, and other software within an IT-based portfolio in order to understand their current condition, to determine cost of operation and support, and to measure their value to current operations. Typically, this analysis becomes a continuous process, regularly monitoring the state of the portfolio as its IT resources and operational objectives evolve.

feasibility, timeliness, and other factors when evaluating ways to migrate current systems to service-oriented capabilities.

Finally, as applications and systems are selected to transition as service providers for C2 capability or to be retired, program and system managers need to develop plans that enable the coordination and synchronization of transition and migration activities. In addition, plans should provide information required to refine and update the CDIs, including end-of-life messages to inform components when capabilities will no longer be supported.

As C2 capabilities evolve toward services-based implementations, the use of enabling services infrastructure from the Net-Centric JCA should replace duplicative functions embedded within individual systems. As users and developers begin to foster a common understanding of key service-oriented design and integration concepts, such as separation of interfaces from implementations or separation of business logic from infrastructure functions, DoD components will need to adapt their training to emphasize the delivery and use of services. Table 4 lists required migration-related implementation activities.

Table 4. Migration-Related Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Conduct rationalization of C2 systems and develop migration/ transition and decommissioning plans for legacy C2 capability.	2.4, 3.6		X			Services DISA	OASD(NII)/ DoD CIO USJFCOM
Develop methods for ensuring C2 capability is sustained throughout the transition to a services-oriented enterprise.	2.4, 3.6		X			OASD(NII)/ DoD CIO	USJFCOM Services DISA

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Develop "To Be" (objective) C2 services-oriented reference architectures and use in development of legacy C2 capability assessment criteria.	3.3, 3.6, 5.2		X			OASD(NII)/ DoD CIO	USJFCOM
Continuously assess alternative system and network implementation strategies through research and development activities, monitoring commercial solutions, Joint Capability Technology Demonstrations, Advanced Concept Technology Demonstrations, Advanced Technology Demonstrations, and prototypes.	2.3, 2.4, 4.5, 5.2	X	X	X	X	USJFCOM	OASD(NII)/ DoD CIO Services DISA

3.2.3 Assured Information Exchange Services

To meet interoperability and collaboration needs, the exchange of C2 information with multinational and interagency mission partners in both optimum and degraded information-sharing environments must be reliable and secure. The DoD Information Sharing Implementation Plan broadly addresses this objective through Task 7.1,[26] and specifically discusses a C2 capability that must provide pervasive and persistent access to multi-level, multi-source data and mission-tailorable services when and where needed by authorized users. Senior leaders, commanders, and staffs must be confident that the security infrastructure and services supporting C2 information sharing ensure data

[26] *DoD Information Sharing Implementation Plan*, April 2009, Task 7.1: "Develop an architecture to converge the multiple secret-level coalition networks into a single mission partner assured information sharing environment, providing a common suite of information services to all mission partners, along with controlled access to command and control, as well as intelligence applications in support of mission planning and execution based on the trust level and duties of the individual user."

integrity and protection and that information exchange protocols and interfaces meet level-of-trust and responsibility-to-provide requirements of mission partners.

Information sharing is enabled by protecting and securing the information being shared and by dividing security into three major areas and systematically tackling each one: empowering unanticipated users, establishing trust across organizational boundaries, and mitigating newly exposed vulnerabilities. The successful delivery of services requires that the right security mechanisms be applied to the right services, balanced with other considerations such as performance and scalability.

To provide pervasive mission partner interoperability and secure horizontal information exchange, today's environment must address several challenges. Bi-directional (high to low as well as low to high) cross-domain solutions that use standards such as XML schema-based guard technology need to mature and become available to programs either as an enterprise or C2-based service.[27] This will address currently deployed, technically diverse cross-domain solutions for well-established structured data. However, these solutions can potentially increase risk due to inconsistent standards application and also cost due to lengthy Certification & Accreditation (C&A) and integration efforts.

DISA's Cross Domain Enterprise Service (CDES) provides service-oriented, cross-domain information sharing solutions. One of CDES's objectives is to consolidate certified cross-domain solutions and to develop cross-domain tools.[28]

To increase the secure flow of horizontal information within the service-oriented C2 environment, metadata schemas will need to specify tag definitions in terms of classification, handling, and verification methods. The Intelligence Community (IC) Metadata Standard for Information Security Marking (IC-ISM) defines the appropriate security tags for information products. This specifies IC handling standards across the full range of security classifications, which enables mission partner information sharing and collaborative environments with disparate classification levels and need-to-know compartments. Table 5 lists required implementation activities in this area.

---

[27] The technologies and standards mentioned in this discussion are current examples of solutions that can support assured information exchange.

[28] Defense Information System Network (DISN): Policy and Responsibilities, July 9, 2008. Two such tools are XML Data Flow Configuration File (DFCF) and Bray.

Table 5. Assured Information Exchange Services Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Develop an Initial Capabilities Document (ICD) for DoD and interagency Cross Domain Services.	2.1, 2.2, 2.3, 2.5, 3.5	X				OASD(NII)/ DoD CIO	Joint Staff Services USNORTHCOM NORAD DISA
Design, develop, and integrate C2 services with appropriate security controls in accordance with enterprise security services and architectures.	2.1, 2.2, 2.3, 2.5, 3.5				X	Services DISA	OASD(NII)/ DoD CIO Joint Staff

3.2.4 C2 in Tactical and Austere Operating Conditions

Whether conducting traditional, irregular, or hybrid warfare operations or other actions, today's operational and tactical environment is characterized by increasingly stealthy, mobile forces widely dispersed upon a non-contiguous battlefield operating at very high operational tempos. Tactical forces frequently operate in disconnected, intermittent, or low bandwidth conditions. These forces may be intentionally "off the net" (e.g., SOF cell), dismounted (out of vehicle operations), or executing decentralized operations consistent with commander's intent. Tactics, techniques, and procedures are part of the solution to mitigate loss of capability, but technical means to ameliorate the effect of DIL conditions also play key roles. The net-enabled warfighter has distinct advantages over his adversary. Given that ubiquitous transport and unlimited bandwidth cannot be assumed in a DIL operating condition, DoD needs robust networks to operate in austere or hostile environments. These include surface, airborne, and space-based networks.

Similarly, overlap of tactical, operational, and strategic levels of war and domestic response increases the need for forces to operate seamlessly across organizational boundaries. Providing C2 capability in such an environment requires a resilient information exchange infrastructure that provides secure and assured situational awareness and understanding from the strategic to the tactical user when and where it is needed. This includes C2 capabilities to share and access information flows across

disparate operational and mission partner organizations in the face of restricted communications, bandwidth limitations, and/or jamming. In addition, information sharing must be provided through consistent end-to-end performance and quality of service (QoS) with as little impact as possible due to austere conditions and diverse operational situations, including weapons of mass destruction (WMD) effects.

Communication infrastructure and systems supporting C2 of lower level tactical units typically do not provide adequate information exchange capacity, especially beyond line-of-sight, and suffer from lack of reliability and periodic loss of connectivity in challenging communications conditions characterized by foul weather, dust and dirt, mountainous and jungle terrains, urban canyons, and a congested electromagnetic environment. Similarly, they do not provide adequate interoperability when supporting civilian partners during humanitarian or DSCA operations. Tactical commanders must not lose the capability to perform core tasks such as planning, transmitting and receiving orders, and updating the common operational picture (COP) when connectivity is lost. Efforts are underway to improve this situation, including development of the Warfighter Information Network – Tactical (WIN-T), Joint Tactical Radio System (JTRS), Joint Aerial Layer Network, Advanced Tactical Data Link Systems (ATDLs), C2 On-the-Move, and the Joint Incident Site Communications Capability (JISCC). There is also the Cryptographic Modernization Plan and supplementing Notice, as well as attempts to place services and data in optimal locations; however, all of these efforts have been slow to develop and communications capabilities at the tactical level continue to be severely constrained. Table 6 lists required implementation activities in this area.

Table 6. Tactical and Austere Operating Conditions Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Ensure future communication systems enhance connectivity, inter-operability, and overall supporta-bility requirements of C2 systems for tactical forces, especially under DIL operating conditions.	2.5		X	X	X	NC CPM Services	OASD(NII)/ DoD CIO DISA Combatant commands CAPE NGB

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Ensure future ISR platforms enhance connectivity, inter-operability, and data integration requirements to meet SA and other C2 capability-based needs.	2.5		X	X	X	Battle-space Aware-ness (BA) CPM Services	OASD(NII)/ DoD CIO DISA NGB

3.3 Implementing Interoperable C2 and Information Sharing with Multinational and Mission Partners

Senior leaders and commanders must be able to achieve and maintain unity of effort by leveraging capabilities of mission partners. Achieving this across the full range of military operations will require C2 capabilities that can support information sharing at both classified and unclassified levels, among own forces, allies, other departments, and with non-traditional partners. Recent experiences with stability and HD-DSCA operations have emphasized the need to share information and capabilities and to collaborate and coordinate actions across a broad spectrum of partnerships.

The DoD Information Sharing Implementation Plan addresses the overarching goals and objectives of the Department in this area. The following paragraphs complement and amplify that guidance specifically regarding information sharing in the C2 domain.

3.3.1 Collaboration and Information Sharing with Multinational and Mission Partners

From a materiel perspective, community focus to date has been on provision of collaboration services at the strategic and higher operational echelons, and on same-network solutions. These solutions tend to be essentially enhanced video-conferencing capabilities that operate well in bandwidth-unlimited situations. Significant needs exist for tactical-level chat capabilities and cross-domain collaboration, both of which are currently being addressed by DoD. Additional emphasis is required in extending these developed capabilities to mission partners, along with the attendant DOT_LPF strategies for enhanced employment. While collaboration services are not addressed within the C2 Portfolio, collaboration policies and procedures and advocacy of C2-specific

requirements will be addressed by the C2 community. Table 7 lists required implementation activities in this area.

Table 7. Implementing Activities to Achieve Net-Enabled Collaboration

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Extend collaboration capabilities to multinational and mission partners for both domestic and overseas operations.	1.4, 2.3, 3.1, 3.2			X		DISA	USJFCOM USNORTHCOM NORAD
Extend collaboration techniques and procedures to multinational and mission partners for both domestic and overseas operations.	1.4, 2.3, 3.1, 3.2			X		USJFCOM USNORTHCOM NORAD	DISA
Create standardized TTP for employment of unique HD-DSCA collaborative capabilities not addressed by the enterprise-level collaborative capabilities TTP implementation activity in Table 1.	1.4, 3.1, 3.2			X		USJFCOM	USNORTHCOM NGB

Assuming that data exists and technically can be accessed by all who need it, the act of sharing data (and information in general) within the Department and with the wide range of mission partners is primarily a series of policy and procedural decisions. The sheer variety in levels of trust, timeliness requirements, and types of coordination means that tiers of partnerships and corresponding policies are needed.[29] Attempts at deriving models for these relationships have been undertaken, but none have been consistently

[29] Policy, responsibilities, and procedures of CJCSI 6510.06A, "Communications Security Releases to Foreign Nations," current as of Jan 11, 2008, must be complied with to accomplish an adequate mission analysis and addresses fundamental materiel solution necessities for conducting multinational and interagency mission partner information exchanges.

adopted. This contributes directly to identifiable deficits in accommodation of multinational and mission partners in collaborative environments.

It is equally important to include mission partner participation in initial planning and mission analysis. It is vital to ensure that C2 capability requirements are based on adequate mission analysis and fully address required needs for all DoD operations with consideration for multinational and interagency mission partners. Specifically, these mission analyses lack a specific, identifiable capability summary reflecting multinational and interagency issues.

Table 8 lists required implementation activities in this area.

Table 8. Implementing Activities to Achieve C2 Information Sharing

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Identify and engage relevant mission partner C2 forums and boards for input to C2 portfolio-based mission analyses.	2.2, 2.3		X			USJFCOM	C/S/As
Expand multinational and interagency partner participation in the C2 CBA process.	2.2, 2.3		X			USJFCOM	Not Applicable

3.3.2 Interoperability with Multinational and Mission Partners

C2 must be accomplished across echelons throughout the joint community and must be interoperable with multinational and mission partners, including those who are unanticipated. As part of DoD's movement toward net-enabled capabilities, multinational and mission partner focus must move from point-to-point interface-based to data strategy and standards-based interoperability. All of this must be accomplished while maintaining information assurance measures, and common technical standards and vocabulary as discussed in Section 3.2.

Greater emphasis must be placed on ensuring bi-directional interoperability with mission partners. Immature plans, standards, and implementation of DoD Net-Centric Data and Services are currently impediments to these interoperability needs. Due to a lack of expandability, scalability, and multi-level security on current C2 systems, as well

as this immaturity, Services and agencies are forging ahead independently with some features that may limit joint interoperability and do not enable mission partner participation to the widest extent practicable.[30]

Multinational information sharing and collaboration is shared with other portfolios. Advocacy for increased participation with multinational efforts and adherence to chosen technical standards will facilitate this goal. Table 9 lists required implementation activities in this area

Table 9. Implementing Activities to Achieve C2 Interoperability

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Ensure that C2 Core development efforts adequately reflect bi-directional information sharing requirements with mission partners.	2.2, 2.3, 3.2		X			C2 CPM	Services DISA
Harmonize C2 Core projects with mission partner agreed-upon data exchange standards.	2.1, 2.3			X		C2 CPM	Services DISA

3.4 Implementing Selected C2 Capabilities

In addition to the more general key actions from the Strategic Plan addressed above, the Strategic Plan included Key Actions to address three specific C2 capabilities that require special attention. These actions address joint fires, combat identification, and FFT at the tactical level; Adaptive Planning and Execution at the strategic and operational levels; and senior leader decision support and SA at the strategic level of military operations and homeland defense.

[30] Policy responsibilities and procedures prescribed in CJCSI 6510.06A, "Communications Security Releases to Foreign Nations," current as of January 11, 2008, must be complied with to minimize impediments to interoperable communications requirements.

3.4.1 Interoperable Command and Control of Joint Fires, Combat Identification, and Friendly Force Tracking

Commanders and other joint, multinational, and mission partner leaders lack fully integrated, interoperable C2 capabilities to provide SA and ensure fires are delivered as needed to maximize combat effectiveness and minimize fratricide and unnecessary collateral damage. C2 of joint fires has improved in many areas, but detailed integration between components and other mission partners (interagency, allies, coalition) is often achieved in an ad hoc manner. Mission partner activity can further complicate the problem. FFT has improved as a result of Service and joint initiatives to increase interoperability. FFT is also of significant value in HD-DSCA operations. However, the ability to provide relevant friendly force SA of ground forces to airborne assets still falls short of the accuracy and timeliness needed to effectively place fires on targets while minimizing risk of fratricide. In addition, land components must still deal with differences in architectures, varying employment concepts based on mission (e.g., hierarchical vs. horizontal), and dissimilar C2 systems, which often lead to bandwidth limitations and network overload. Finally, although DoD has made progress in CID, the combined force situation with mission partners is not progressing as fast as is needed.

CID is achieved through a combination of SA + Target Identification (cooperative and non-cooperative), refined through doctrine, the rules of engagement, and the TTPs used, and is not achieved purely through digital means. Although Army and Marine forces involved in current operations are temporarily equipped with common C2 (specifically SA) equipment, they have historically employed technically disparate and non-interoperable systems, hindering the conduct of lower-level ground operations. This problem may be compounded when taking into account the potentially varying C2 modalities of the reserve components. Joint solutions that can be implemented in all operational domains are required to address these issues. For example, in accordance with a series of JROC Memoranda dating to 2003, and in coordination with the Combat Identification / Blue Force Tracking Executive Steering Committee (CID/BFT ESC) and the Army-Marine Corps Board (AMCB), the Services are pursuing a joint solution that includes not only interoperable equipment but common security policies, TTPs, and data approaches. The solution will evolve over time and is expected to be fielded on platforms (e.g., tactical vehicles) by FY2013 and be available for training in Tactical Operations Centers and Combat Operations Centers (TOCs/COCs) by 2015. This evolutionary plan needs to be vigorously pursued.

Addressing the problems above requires common awareness/understanding of technology-ready interoperable capabilities that can be enabled or enhanced by employing current architectures, refined TTPs, and improved training to optimize usage and benefit of "As-Is" technology. Specific attention should be given to sustained development and procurement of previously identified solutions, compliance with previous C2 CPM prescriptions, cross-portfolio coordination for data provision, and synchronization of fielding activities. Key to implementation of the Joint Fires, CID, and FFT-related objectives are the JROC-chartered Joint Fires Support (JFS) Executive Steering Committee (ESC) and CID-BFT ESC.[31] The ESCs are important joint forums for coordinating C/S/A actions toward achieving integrated, interoperable capabilities supporting these mission areas. The ESC-action forums develop, publish, conduct, and update action plans that are aligned with DoD C2 priorities and make recommendations to the JROC. The ESCs function as important vetting venues for CID, FFT, and Joint Fires/Joint Close Air Support (JCAS) issues of interest to the Department.

Table 10 lists the major implementation activities to be undertaken to achieve this key action.

Table 10. Joint Fires, Combat ID, & Friendly Force Tracking Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Complete the Draft CID-BFT JCD and Joint Close Air Support JCD.	1.1	X				USJFCOM	Services
Integrate Joint Fires, Combat Identification, and Friendly Force Tracking training and TTPs across both joint and multinational partners.	1.1		X			USJFCOM	Services

[31] See "Joint Capabilities Document (JCD) for Combat Identification - Blue Force Tracking (CID-BFT)," April 10, 2009.

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Converge Land Component C2/SA to achieve interoperable capability (Platform), Squad Leader through Brigade/Regiment.	1.1			X		Army USMC	OASD(NII)/ DoD CIO USJFCOM
Converge Land Component C2/SA to achieve interoperable capability at Command Posts (TOC/COC).	1.1				X	Army USMC	OASD(NII)/ DoD CIO USJFCOM
Synchronize fielding and integration of Mark XIIA Mode 5 IFF capability (IOC).	1.1			X		Services	OUSD(ATL) OASD(NII)/ DoD CIO USJFCOM
Develop, fund, and field coordinated implementation of Digitally-aided CAS (DaCAS) capability.	1.1				X	Services	OUSD(ATL) OASD(NII)/ DoD CIO USJFCOM
Provide FFT Situational Awareness for the HD and civil support (CS) operational picture and information sharing environment.	1.1	X	X			USNORTHCOM	NGB

3.4.2 Adaptive Planning and Execution

The demands of homeland and global operations warrant revisions to the current planning and execution paradigm now in use across most of DoD. The accelerated pace and complexity of military operations requires commanders to have the ability to respond quickly to dynamic threats and challenges. The fluid and uncertain international situation requires a transformed planning and execution approach across the DoD, which quickly generates and/or updates detailed contingency plans containing multiple options that can be readily adapted to the given circumstances and then rapidly transitioned to execution. This enhanced planning and execution process is Adaptive Planning and Execution (APEX), the goal of which is to align and synchronize the adaptive planning process with other functional activities, such as intelligence, logistics, force management, and force employment. APEX seeks to provide the C/S/A and the Joint Staff with an aligned end-

to-end process, integrated with multinational partners and U.S. Government departments and agencies, as required, and facilitated by trained personnel and technology.

The AP Roadmap II[32] continues the Adaptive Planning (AP) Initiative by building on the groundwork laid by the first Adaptive Planning Roadmap. Initial implementation is ongoing and will focus on achieving an improved transition from planning (contingency and crisis) to execution. The Roadmap provides guidance for improvement and support for the AP initiative across DOTMLPF.

A key process for APEX is course of action (COA) development. The Integrated Strategic Planning and Analysis Network (ISPAN) has been designated as the program of record for joint COA development at the combatant command/strategic level. As such, it is intended that services developed under the ISPAN program be made available to the DoD Enterprise.

An ongoing effort supporting several APEX initiatives is the Global Force Management Continuous Process Improvement (GFM CPI) (formerly called the Force Management Integration Project [FMIP]). The GFM CPI effort will develop and execute a plan to integrate and synchronize policy, processes, authoritative databases, and technology affecting AP, Joint Force Providing, and Joint Deployment to enable more coherent, effective, and efficient GFM.

Table 11 lists the C2 implementation activities for Adaptive Planning and Execution.

Table 11. Adaptive Planning & Execution Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Complete As-Is APEX Architecture to support future APEX implementation.	1.2		X			USJFCOM	Combatant commands USD(P) Joint Staff DISA
Complete APEX ICD.	1.2	X				USJFCOM	C/S/As

[32] "Adaptive Planning Roadmap," Adaptive Planning Executive Committee, March 2008

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Complete ISPAN Increment II-III CDD.	1.2		X			USSTRATCOM	USJFCOM USAF
Support GFM CPI in synchronizing GFM policies, processes, and technology efforts.	1.2	X	X	X	X	USJFCOM DISA	USSOCOM
Demonstrate the interoperability and data sharing required to enable planning services, force sourcing services [Joint Capabilities Requirements Manager (JCRM)], and the deployment execution service [Joint Operation Planning and Execution System (JOPES)], to exchange data. Also, provide interoperable improvements to JCRM and Logbook tools to demonstrate a collaborative staffing ability. [AP Pilot-Global Force Management Planning and Execution (GFMPEX) JCTD].	1.2		X			USJFCOM	OASD(NII)/ DoD CIO
Demonstrate interoperable joint/ coalition geo-enabled C2 enterprise information solution to achieve unity of adaptive planning and execution among C2 partners. (Common Ground JCTD).	1.2		X			USJFCOM	OASD(NII)/ DoD CIO

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Demonstrate an integrated, open-source, spatially/ relationally/temporally referenced human terrain data collection and visualization toolkit that helps combat teams understand the cultural context in which they must operate. Optimize the commander's operational decision-making process in a way that best harmonizes unit actions with the local culture. (Mapping the Human Terrain JCTD).	1.2		X			OUSD(AT&L)	Combatant commands OUSD(P) OUSD (I) OASD(NII)/ DoD CIO Joint Staff DISA

3.4.3 National and Nuclear Command Capabilities (Senior Leader C2)

This C2 capability addresses several overlapping mission areas characterized as National, Nuclear, and Continuity of Government (COG), which range from nuclear C2, to senior leader C2, to C2 support for missile defense, to providing policy for COG communications. To protect our national interests, national leaders require global situational understanding, the ability to deliberate, review options, and make time-critical decisions in response to national-level events.

Traditionally, nuclear C2 depends on closed systems that are platform-centric and hardware-based. The present focus is to migrate selected non-survivable systems to an IP-based approach while preserving the high-assurance, robust, and survivable C2 capabilities required by national policy and to adapt some single-focus systems, where appropriate, to support non-nuclear situations.

In support of National Security/Emergency Preparedness (NS/EP) and DSCA, challenges revolve around achieving interoperability to include improving communications interoperability between DoD and its mission partners.

Within the COG domain, the emphasis is on defining a secure, integrated COG communications capability for the President of the United States (POTUS), Vice President of the United States (VPOTUS) and category 1 executive departments and

agencies—a DoD responsibility under NSPD-51/HSPD-20. Key COG enablers are: Senior Leader Command, Control and Communications System (SLC3S), National Military Command System (NMCS), Nuclear Command and Control System (NCCS), Nuclear Command, Control and Communications—Long Term Solution (NC3 LTS), Defense Continuity Integrated Network (DCIN), and Service Oriented Architectures (SOA)/Net-Centric Data Strategy (NCDS).

The key action encompasses fielding C2 capabilities for Senior Leaders at any location and in any environment, providing discussion/decision support services, providing capabilities enabling the New Triad, and providing DoD capabilities to ensure continuity of operations (COOP) and COG. Assured information sharing between national and DoD systems is a key enabler for these capabilities.

Table 12 lists the implementation activities to be undertaken to achieve this key action.

Table 12. Senior Leader Support Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Develop a Concept of Operations and Implementation Strategy for COG communications, for which the DoD has the lead per NSPD 51/HSPD 20.	1.3		X			OASD(NII)/ DoD CIO	Not Applicable
Continue development of the NMCS Transformation CONOPS. The NMCS is the survivable core of the DNLCC, and the Transformation CONOPS sets out the purpose, assumptions, constraints, goals, and relation to the DNLCC.	1.3		X			Joint Staff	Not Applicable

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Develop a strategy to provide, regardless of location or environment, integrated information and robust command capability for DoD & national leadership planning and decision making.	1.3			X		OASD(NII)/ DoD CIO	Not Applicable
Develop a framework (decision forum/process) to achieve interoperable C2 across Senior Leader, New Triad (global strike), nuclear, COOP/ COG/ECG and national mission areas.	1.3			X		OASD(NII)/ DoD CIO	Not Applicable

4. IMPLEMENTING C2 GOVERNANCE AND C2 CAPABILITY PORTFOLIO MANAGEMENT

This section provides guidance for implementing C2 governance and management activities and processes. Section 4.1 below addresses C2 portfolio governance and management activities in general including C2 CPM externally focused management activities. Section 4.2 addresses focused C2 CPM management activities.

4.1 Approach for Governance and Management of C2 Implementation Activities

Synchronizing the implementation of C2 capabilities requires a common framework within which all C2-related JCIDS, PPBE, and DAS activities are conducted and managed. As discussed in the DoD C2 Strategic Plan and in Section 2.3 of this plan, that framework must incorporate CDIs with metrics to enable designated governance and management bodies to monitor progress and direct adjustments in executing essential supporting strategies and approaches (e.g., DoD's Net-Centric Data and Services strategies) that enable attainment of DoD C2 Strategic Plan objectives. Appropriate Service plans must be synchronized with DoD-wide C2 implementation planning as well as implementation plans of enabling capability portfolios.

The integration of C2-related activities within and across institutionalized DoD capability-related processes is depicted conceptually in Figure 1 of the DoD C2 Strategic Plan as a point of departure for developing more detailed processes and approaches to enable effective governance and management of implementation activities across the C2 capability portfolio.

Figure 4 depicts a conceptual framework for integrating and synchronizing the implementation activities identified in this plan. It suggests that all C2 implementation activities, from the perspective of portfolio management, can be related to one or more of the following five overarching activities: (1) DoD Vision and Strategic Goals, (2) Capability Needs Definition Processes, (3) Resource Allocation Processes, (4) Program Definition and Execution, and (5) Rapid Capability Insertion Processes. The conceptual framework highlights the interfaces (i.e., information inputs or interactions) between the major activities (the arrows crossing between the blocks in the figure) which, in most cases, consist of documents or products that move between and among management entities. Improving the quality and timeliness of these information exchanges will

contribute directly to more effective governance and portfolio management for C2 capabilities. This framework is consistent with governance and management imperatives provided in the DoD C2 Strategic Plan.

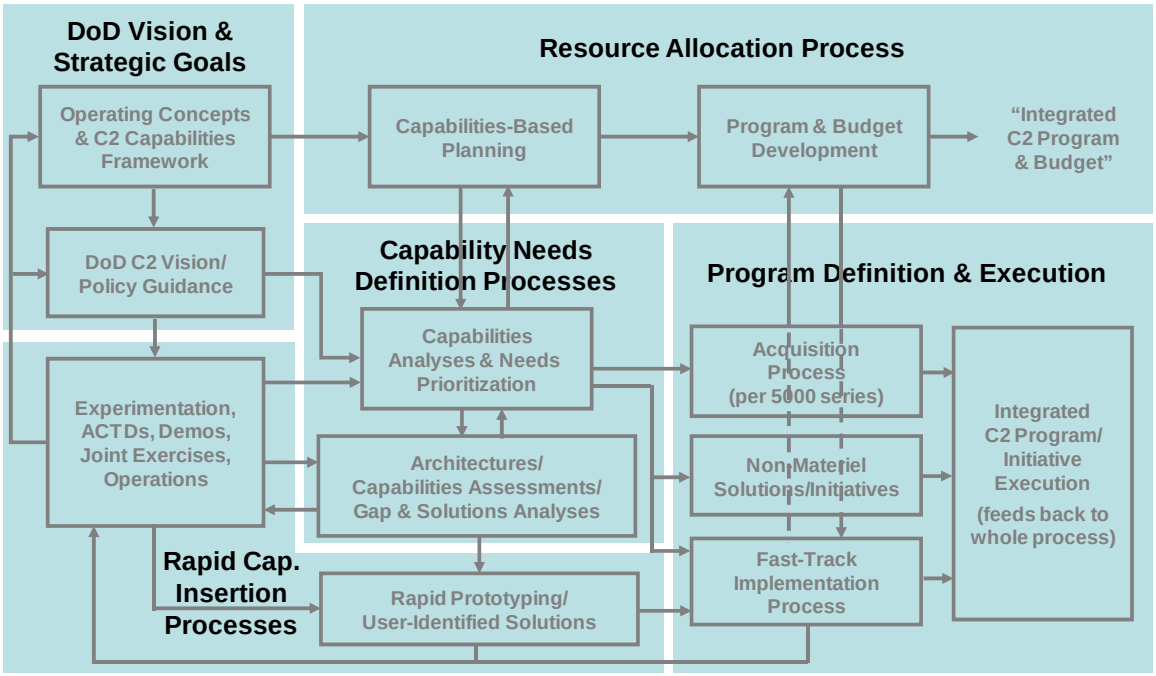

Figure 4. Conceptual Framework for Governance and Management of C2 Implementation Activities

DoD C2 capability governance and management is based on established roles and responsibilities specified in the Unified Command Plan (UCP), in existing DoD policy, or in statute. These include, but are not limited to, CJCS responsibilities as the Principal Military Advisor (PMA) for DoD C2; OASD (NII)/DoD CIO responsibilities as the Principal Staff Assistant (PSA) for DoD C2; and C2 capability portfolio management responsibilities assigned to USJFCOM, OASD(NII)/DoD CIO, and the Joint Staff J3; and the Services' Title 10 responsibilities to organize, train, and equip. Overall responsibility for C2 implementation activity oversight and integration rests with the C2 CIB and the enabling DoD C2 governance and management structure as described in the DoD C2 Strategic Plan. The C2 CPM and the C2 SWarF perform key roles in supporting the C2 CIB in the execution of this responsibility. Accordingly, to help further define and institutionalize effective portfolio management practices, the C2 CPM will explore alternative approaches to oversee and integrate C2 planning and implementation activities

(to include the development of specific management processes where applicable) and recommend a preferred overall approach for C2 portfolio management to the C2 CIB. In particular, it is necessary to coordinate and synchronize the governance and management activities currently required to support C2 CIB capability portfolio management responsibilities with those that support Joint Staff information technology portfolio management responsibilities.[33] It is also important to address cross-portfolio coordination—particularly between the C2 CPM and the NC, BA and Logistics CPMs. Finally, the recommended approach for achieving oversight and synchronization should include a means for a periodic review of progress in completing all implementation activities addressed in this DoD C2 Implementation Plan. The implementation activity in Table 13 addresses this need.

Table 13. C2 Portfolio Management Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Identify mechanisms and procedures to synchronize and coordinate IT portfolio management and capability portfolio management activities as prescribed in DoDD 8115.01, Information Technology Portfolio Management, and DoDD 7045.20, Capability Portfolio Management, respectively, so that corresponding C2 portfolio management and governance activities conducted in compliance with these two directives are complementary and mutually supporting.	4.1, 4.5	X				OASD(NII)/ DoD CIO	OUSD(P) Joint Staff USJFCOM

[33] These responsibilities are prescribed in DoDD 7045.20, "Capability Portfolio Management," and DoDD 8115.01, "Information Technology Portfolio Management," respectively.

4.2 C2 Capability Portfolio Management

4.2.1 C2 Capability Development Organization, Processes, and Policy

Implementation planning is primarily facilitated by the C2 CPM under the general oversight of the ASD(NII)/DoD CIO, the PSA for DoD C2, in collaboration with the combatant commands, Services, agencies, other offices in OSD, and the Joint Staff. Portfolio management direction and guidance for the Department is consolidated in DoDD 7045.20, "Capability Portfolio Management." While portfolio managers have no independent decision-making authority, they are responsible for working within established coordination processes and appropriate forums to identify issues, priorities, and capability and resource mismatches (gaps, shortfalls, and redundancies). The C2 CPM organization is headed by a Government civilian co-lead, the ASD(NII), and a military co-lead, Commander, USJFCOM. The Joint Staff OPR for the C2 Portfolio is the Director for Operations (J3). USJFCOM is further empowered to inform the C2 requirements process through JROC-delegated C2 Joint Capabilities Board (JCB) authorities.

Three overarching principles will guide effective implementation activities:

- Collaboration among combatant commands, Services, agencies, CPMs, and mission partners facilitated by information and process access and transparency
- Consensus building using established Departmental coordination processes and extant governance and management to identify and prioritize C2 capabilities
- Compelling logic based on adequate risk-based analysis, incorporating considerations for multinational and interagency partners.

The C2 CPM provides specific recommendations and advice to DoD decision makers and forums regarding integrating, coordinating, and synchronizing capability requirements with capability investments. Analyses based on detailed review of DoD strategic guidance and current C/S/A capability issues support these recommendations. Portfolio analyses incorporate detailed review of guidance, determination of specified and implied tasks, and needs and requirements review to fully understand and consolidate capability issues. Risk considerations and capability priorities recommendations are provided to the C2 SWarF, the Joint Staff, and other appropriate forums for consideration in capability attribute development and the prioritization of capabilities.

The CPM has established C2 integrated architectures and data implementation approaches supporting C2 capabilities among critical activities. Collaborative forums, including the Joint Architecture Integration Working Group (JAIWG), Joint Fires Support ESC, C2 Capability Portfolio Data and Services Steering Committee (DSSC), and other working groups are established to advance enterprise areas and address key implementation actions.

More remains to be done to advance CPM planning and management and to support C2 capabilities based on given warfighter priorities, C/S/A plans, and known resource constraints. In the C2 policy area, continuing effort is required to achieve a concise and coherent set of OSD policy guidance to enable planning and execution. Policy review should span the entire C2 capability area to support clear policy that enables identification and prioritization of combatant command C2 requirements, integrated with the Services' needs. Also, the Services must have clear technical guidance for C2 capabilities. Improved coordination with multinational and non-military/civil entities is essential for effective mission integration. Table 14 lists the implementation activities to address C2 CPM organization, processes, and policy issues.

Table 14. C2 Capability Development Organization, Process, & Policy Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Establish and maintain comprehensive and clear technical standards policy to ensure unity of effort across DoD for C2 capability development, acquisition, fielding, and sustainment.	5.6		X			OASD(NII)/ DoD CIO	Joint Staff USJFCOM DISA
Refine the Net-Ready Key Performance Parameter, with the additional use of universal joint tasks, to enhance interoperability testing and certification.	5.5	X				USJFCOM	OASD(NII)/ DoD CIO Joint Staff

4.2.2 C2 Capability Development and Delivery

C2 capability portfolio management must support definition and implementation of development approaches that sustain incremental delivery of C2 capabilities across a distributed development environment. A need exists for more agility in C2 capability implementation. C2 capability development must be more responsive to the needs of leaders in the field.

Development of a persistent test and assessment environment is key to achieving that responsiveness and agility. The environment will include operational expertise, technical expertise, infrastructure (including networks, systems, test tools), and scientific methodologies. Current testing and evaluation approaches are organized to support programs with defined deliverables and end-states. They do not provide agile engagement for emergent and user developed capabilities in a mission context. The lack of persistent and accessible test resources imposes barriers to conducting timely and effective operational evaluations of capabilities realized by composition of multiple systems from multiple providers. A persistent C2 test and assessment environment will provide a readily available, robust distributed environment that links a large number of diverse material and human resources. It will also allow for continuous assessment using available infrastructure and provide a bridge between the current environment and net-enabled development activity. In addition, by facilitating Service program assessment in a joint operational environment, it can provide the insight necessary to ensure C2 capabilities are "born joint."

The C2 CPM is committed to managing time-phased evolution of capabilities through CDIs. Although the CDIs are still being formulated and require additional quantification and qualification, they provide an initial mechanism for informing governance and management recommendations for C2 operational capabilities between 2010 and 2020. The CDIs also provide a means to evaluate progress towards objective C2 capabilities, applying the JCA framework and lexicon.

To satisfy their intended purpose, CDIs should be operationally useful, technically feasible, programmatically achievable, and fiscally affordable. Table 15 lists the implementation activities to be undertaken to address C2 capability development and delivery issues.

Table 15. C2 Portfolio Capability Development & Delivery Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Provide a C2 persistent test and assessment environment that leverages existing labs, test facilities, and operational infrastructure.	4.4, 5.5		X			USJFCOM	DOT&E C/S/As Joint Staff
Synchronize CDIs with other capability portfolios (C2 and NC CPM; others to follow).	4.1, 5.3		X			C2 CPM	Other CPMs
Develop quantified & qualified CDIs; include assessment of risk factors. Develop a CDI evaluation strategy.	3.3, 4.3		X			C2 CPM	C/S/As

4.2.3 C2 Portfolio Risk Assessment

Risk assessment must be integral to all aspects of C2 capability portfolio management. The DoD C2 Strategic Plan notes that operational risk remains the primary basis for allocating resources to develop, field, and sustain C2 capabilities. However, programmatic risk calculations are supported by management processes that allow warfighters/developers/managers to collaborate on cost, schedule, and risk tradeoffs throughout a program life cycle. A major theme in the operational risk area is "Do no harm"—no loss of current operational capabilities during the transition to future capabilities. Accurate prioritization of C2 capabilities is not possible without an effective risk assessment mechanism. The C2 CPM will develop and recommend to the C2 Capability Integration Board (C2 CIB) appropriate procedures and mechanisms for obtaining and considering risk estimates or assessments from the warfighter community. Table 16 lists the implementation activities to be undertaken to address risk assessment.

Table 16. C2 Portfolio Risk Assessment Implementation Activities

Implementation Activity	Relevant Key Action	2010	2012	2014	2016	OPR	OCR
Establish a mechanism for review/maintenance/ evaluation of C/S/A migration plans.	5.4	X				C2 CPM	C/S/As Joint Staff
Using appropriate forums, such as the C2 SWarF, ensure that the warfighting community's risk estimates and/or assessments are integral to the C2 portfolio analysis process and, where appropriate, address capability attribute development efforts and capability prioritization.	4.2	X				USJFCOM	OASD(NII)/ DoD CIO Joint Staff C/S/As NGB

Appendix A
DOD C2 STRATEGIC PLAN OBJECTIVES AND KEY ACTIONS ANALYSIS

1. DOD C2 STRATEGIC PLAN OBJECTIVES AND KEY ACTIONS

The C2 Strategic Plan identifies and discusses five overarching C2 objectives and 27 key actions related to those five objectives. Table A1 lists the DoD C2 Strategic Plan objectives and their corresponding key actions.[34]

Table A1. Strategic Plan C2 Objectives and Key Actions

Strategic Plan Objective	Strategic Plan Objective Key Actions
Objective #1: Provide the capabilities necessary to effectively support organizing command structures and forces, understand situations, plan and decide upon courses of action, and direct and monitor execution across the range of DoD operations.	1.1: Provide C2 capabilities that support joint fires, combat identification and friendly force tracking, and common tactical information capabilities that are interoperable with mission partners. 1.2: Mature the integration of adaptive planning and execution capabilities with readiness, global force management, and intelligence capabilities to enable the Department to leverage all DoD assets, the instruments of national power, and contributions of mission partners to achieve national, theater, tactical, and multinational objectives. 1.3: Provide national senior leadership ready access to global situational awareness (SA) and the ability to discuss options and make decisions in response to events. This reduces the time to understand a situation but increases the time available to respond to an increasingly complex and evolving set of strategic challenges. 1.4: Enhance and manage classified and unclassified collaborative capabilities to organize, understand, plan, decide, direct, & monitor operations. 1.5: Accelerate the transformation of designated existing service operational headquarters to fully functional and scalable joint command and control joint task force-capable headquarters.

[34] The key action numbers in Table A1 are not used in the C2 Strategic Plan. They are inserted here only for convenience in linking the DoD C2 Implementation Plan implementation activities (contained in the 16 Section 3 and 4 tables) to specific DoD C2 Strategic Plan key actions.

Strategic Plan Objective	Strategic Plan Objective Key Actions
Objective #2: Enable military forces and mission partners to conduct integrated operations across the range of DoD operations at all echelons of command.	2.1: Enable integrated operations through joint common mission applications, joint data interoperability and/or standardization and, where required, cross-security domain data. 2.2: Ensure that C2 capability requirements are based on adequate mission analysis and fully address required needs for all DoD operations with consideration for multinational and interagency mission partners. 2.3: Increase emphasis on integration and interoperability of C2 capabilities with mission partners with specific emphasis on multinational and interagency sharing of information and services to promote employment of the full range of forces and options available. 2.4: Enable the Services to retire all or portions of stove-piped legacy C2 systems (and replace) with more interoperable and integrated joint Service capabilities without losing any current capability relevant to Service missions. 2.5: Provide robust and resilient C2 capabilities that are available across all operating environments to include low-bandwidth, degraded, and disconnected communications environments.
Objective #3: Maximize assured sharing of information and services and synchronized implementation of collaborative C2 capabilities.	3.1: Implement cross-Service DOTMLPF approaches to leverage and standardize TTPs for employment of collaborative capabilities. 3.2: Achieve collaborative capabilities that enable interoperable, integrated visualization and manipulation of the relevant operational environment and the subsequent sharing of SA among all mission partners including, where necessary, interagency partners and allies. 3.3: Streamline the myriad architectures addressing the DoD C2 space and clarify the requirements and methodologies to better support and guide the joint integration of development efforts. 3.4: Define a DoD Net-Centric Data and Services Strategy implementation approach for DoD-wide C2 capabilities. 3.5: Ensure that C2 applications and services are accessible and robust and consistent with related network information assurance initiatives. 3.6: Migrate, where applicable, C2 capabilities towards joint programs and increase the use of common infrastructure-based services being developed expressly for that purpose.
Objective #4: Optimize C2 capability investments across the range of DoD operations.	4.1: Implement capability portfolio management that is responsive to emergent senior leader and warfighter requirements while addressing long-term capability objectives across the spectrum of DoD capabilities. 4.2: Implement CPM-facilitated risk-based analysis processes that identify areas to reduce risk, hold risk constant, or accept risk for operational forces. 4.3: Develop and appropriately resource prioritized and integrated C2 CDIs. 4.4: Define and implement development approaches that support incremental delivery of C2 capabilities across a distributed development environment. 4.5: Work within the JCIDS, PPBE, and DAS processes to identify C2 capability needs, influence the allocation of resources, and acquire required C2 capabilities.

Strategic Plan Objective	Strategic Plan Objective Key Actions
Objective #5: Achieve agile and responsive development, acquisition, fielding, and sustainment of C2 capabilities across the DOTMLPF spectrum.	5.1: Develop additional C2 education and training across the Department as a principal means of increasing the quantity and quality of jointly trained C2 practitioners. 5.2: Accelerate the transition from traditional, Service-centric and other non-interoperable C2 capabilities to joint net-centric capabilities to include implementation of service-oriented architectures, enterprise-based C2 capabilities, and supporting data and service strategies where achievable. 5.3: Implement a process to identify and update, as required, C2 CDIs that are synchronized and federated with delivery of enabling capabilities from other capability portfolios. 5.4: Implement component and C2 CPM plans and programs that support development, acquisition, fielding, and sustainment of capabilities in support of DoD C2 objectives. 5.5: Streamline and accelerate current test and evaluation processes and planning cycles to better support responsive development, acquisition, and fielding of C2 capabilities. 5.6: Identify and update, as required, the policies needed to ensure unity of effort across DoD for development, acquisition, fielding, and sustainment of DoD C2 capabilities.

2. IDENTIFYING AND ORGANIZING IMPLEMENTATION ACTIVITIES

Figure A1 depicts at a high level the process by which C2 implementation activities were identified and are expected to be updated and refined over time. Note the inclusion of the CDI and OCMS efforts referred to in Section 2.3. Beginning on the left with the C2 Vision, the DoD C2 Strategic Plan provides DoD's C2 capability objectives and then identifies associated key actions to achieve those capability objectives. The common lexicon for discussion of C2 capabilities is provided by the C2 Joint Capability Areas (JCAs). Moving from left to right across the diagram, qualitative and quantitative understanding of the key actions is informed by the CDIs, OCMS, JFCOM CBA results, and other supporting analyses, Service migration plans, and relevant operational and systems architectures. As noted in Section 2.3, this end-to-end process is envisioned to be much more robust in support of future updates to the DoD C2 Implementation Plan than was possible for the current version. However, in support of the current version, key *enablers* were identified for each key action and then aggregated into *implementation themes*. (This process is described in greater detail below.) Finally, stakeholder input and reviews (not shown in Figure A1) were critical to identifying and refining all required implementation activities.

DoD C2 implementation must remain consistent with and be within the context of current DoD policies, planning, programming, concepts, and other guidance. The DoD

C2 Implementation Plan should inform development of the other documents, consistent with effective dates. This requires a continuous effort to ensure that all C2 guidance is issued with the necessary degree of top down consistency so that C2 planning and implementation activities are consistent and mutually supporting.

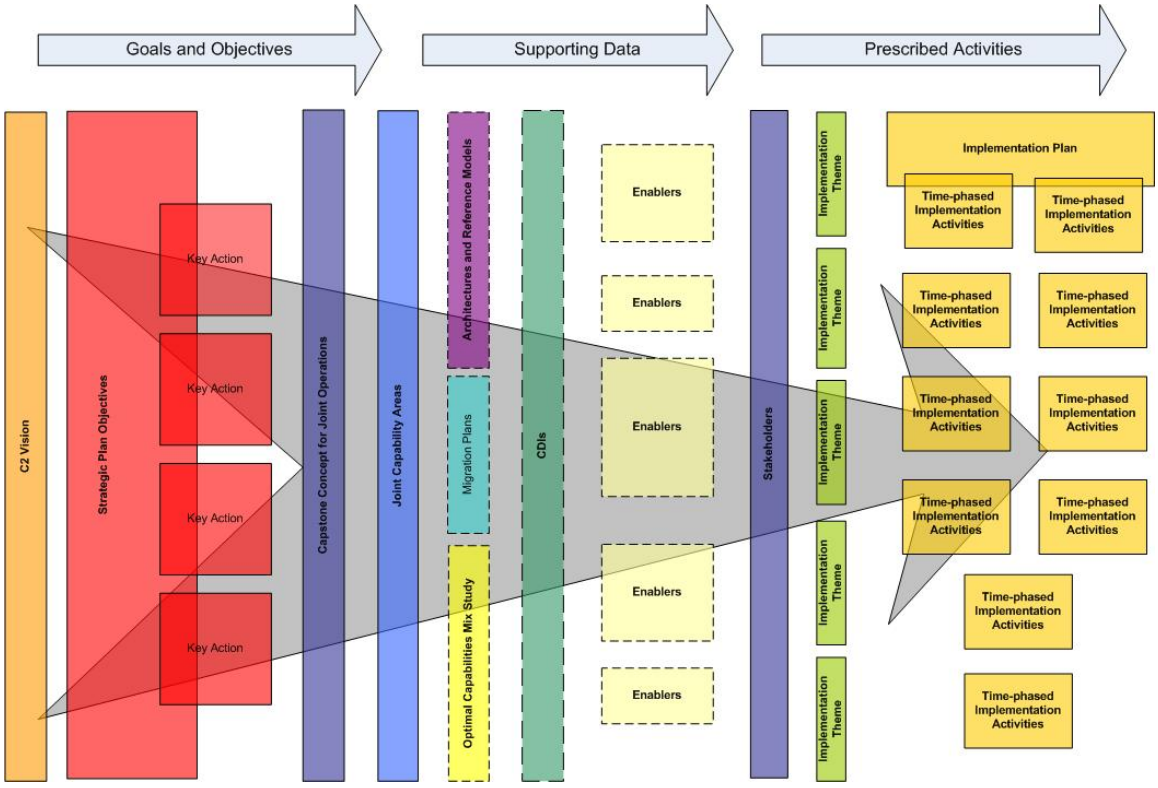

Figure A1. Identifying C2 Implementation Activities

Referring to the need for *implementation themes*, the DoD C2 Strategic Plan objectives and key actions are intentionally characterized as broad, capability-based concepts as seen from the perspective of the joint warfighter. They are, therefore, inherently wide-ranging and multi-dimensional in nature and, in some cases, contain or imply duplicative or overlapping component capabilities. An analysis of the 27 key actions in terms of *enablers* and *implementation activities* (these terms are defined below) shows a fair amount of commonality and interdependence. Therefore, an implementation framework based solely on the organizational construct of the DoD C2 Strategic Plan objectives and key actions would potentially contain significant redundancies. Accordingly, from an implementation perspective, it is useful to begin with an understanding of the objectives and key actions but then to shift to a C2 implementation

construct that is better suited for identifying implementation activities and assigning responsibilities for their execution.

Figure A2 depicts the process of analyzing the key actions identified in DoD C2 Strategic Plan and deriving corresponding *C2 implementation themes*. The key action analysis addressed the following topics:

- Focus/Major Thrust: what this key action is intended to achieve.
- Significant Gaps/Deficiencies: the gaps or process deficiencies that give rise to this key action.
- Discussion: context and explanation of the proposed way ahead for achieving the needed capability or process improvement.
- Key Enablers: a list of the most important materiel and/or non-materiel enablers needed to accomplish this Strategic Plan key action.

An "enabler" is any materiel and/or non-materiel "provider" of capability that partially or fully satisfies the operational needs articulated or implied in the key action. An enabler can be a program, system, development effort, technology, COI, analysis, TTP, doctrine, training initiative, management process, or any other effort leading to partial or full satisfaction of the key action.

- Key Implementation Activities: the most important, potentially high-payoff implementation activities to be executed over the four timeframes of interest (i.e., by 2010, 2012, 2014, or 2016).

"Implementation Activities" are activities, actions, or events necessary to accomplish the key action.

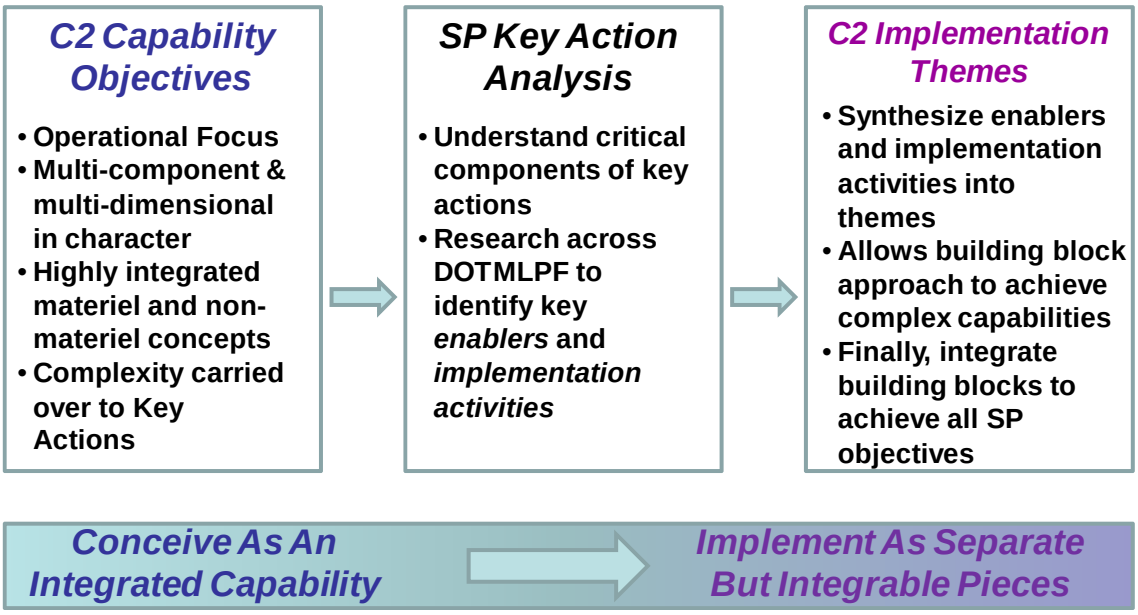

Figure A2. C2 Capability Objectives and Implementation Themes

As shown in Figure A2, the results of the key action analysis were used to identify focused implementation themes within which implementation activities can be organized. These implementation themes, when implemented collaboratively, will facilitate unity of effort in achieving DoD C2 Strategic Plan objectives. The five implementation themes identified in this analysis and codified in this plan are as follows:[35]

- Achieving Leader-Centric C2 (key actions 1.5, 5.1)
- Implementing Net-Enabled C2 Capabilities[36] (key actions 2.1, 2.4, 2.5, 3.3, 3.4, 3.5, 3.6, 5.2)
- Implementing Interoperable C2 and Information Sharing among U.S. Forces and Multinational and Interagency Mission Partners (key actions 1.4, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 3.4)
- Implementing Selected C2 Capabilities

---

[35] Refer to Table A1 to correlate the key action numbering shown with each theme with the actual key actions that are articulated in the C2 Strategic Plan.

[36] As stated in paragraph 2.2, the term "net-enabled" is used here in its most generic context—i.e., C2 operations facilitated through the use of information technology (IT) systems interconnected via a communication network or network of networks. In terms of technical implementation, it is understood that the term "net-enabled" often has a much more specific meaning—i.e., the ability of an application, system, or function to be accessed and used via an IP-based network (vice a local client); or to characterize an incremental step in system development such as that from client-server-based capability to net-centric or SOA-based capability.

  - Implementing Interoperable C2 of Joint Fires, Combat Identification (CID), and Friendly Force Tracking (FFT) Capabilities *(key action 1.1)*
  - Implementing Adaptive Planning and Execution *(key action 1.2)*
  - Implementing National and Nuclear Command Capabilities (Senior Leader C2) (key action 1.3)
- Implementing C2 Portfolio Management (key actions 3.3, 4.1, 4.2, 4.3, 4.4, 4.5, 5.3, 5.4, 5.5, 5.6)

(This page is intentionally blank.)

Appendix B
DEFINITIONS AND ACRONYMS

DEFINITIONS

Accessibility: The ability of all levels of command (strategic, operational, and tactical) to pull or push relevant data and information that are the basis for shared situation awareness. Additionally, access to a standardized joint application tool set from garrison to forward deployed locations will drive the ability to increase decision-making capabilities supporting rapid, efficient, effective command and control. [*C2 JIC*]

Adaptive Planning (AP): The joint capability to create and revise plans rapidly and systematically as circumstances require. Adaptive Planning occurs in a networked, collaborative environment, requires the regular involvement of senior leaders, and results in plans containing a range of viable options.

Agility: The ability to respond effectively and in a timely manner to changing circumstances. Agility includes both "flexibility" and "responsiveness." [*C2 JIC*]

C2 Core: A decentralized run-time set of infrastructure capabilities that provide the necessary common facilities for sharing information required to command and control forces. The C2 Core is comprised of the following artifacts: a Joint C2 Conceptual Model and Vocabulary, C2-specific Extensions from the UCore, the C2 Information Sharing Framework (operational data infrastructure available at the run-time level), and C2 Core Service Specifications.

Capability: The ability to achieve a desired effect under specified standards and conditions through a combination of means and ways across doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) to perform a set of tasks to execute a specified course of action. [*DoDD 7045.20*]

Capability Portfolio Management: The process of integrating, synchronizing, and coordinating Department of Defense capabilities needs with current and planned DOTMLPF investments within a capability portfolio to better inform decision making and optimize defense resources. [*DoDD 7045.20*]

Capability Portfolio Manager (CPM): The civilian and military co-leads accountable for the execution of capability portfolio management activities for a defined portfolio. [*DoDD 7045.20*]

Capability Portfolio Strategic Plan: The CPM's long-range plan to synchronize, integrate, and coordinate efforts related to capability investments to meet joint warfighter and supporting defense entity needs. These plans address portfolio scope, portfolio objectives, dependencies with other portfolios, processes and plans, performance targets and metrics, and risk considerations. [*DoDD 7045.20*]

Collaboration: Joint problem solving for the purpose of achieving shared understanding, making a decision, or creating a product across the Joint Force and mission partners. [*NCE Joint Functional Concept*]

Collaborative Information Environment (CIE): Generally defined as a virtual aggregation of people and organizations, infrastructure, and policy and procedures to create and share the data, information, and knowledge needed to plan, execute, and assess operations and to enable a commander to make decisions better and faster than the adversary. [JP 6-0, Joint Communications Systems; JP 2-0, Joint Intelligence; and JP 3-57, Civil-Military Operations, among others]

Command and Control (C2): The exercise of authority and direction by a properly designated commander over assigned and attached forces and resources in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. [*JP 1-02*]

Commander's Intent: A concise expression of the purpose of the operation and the desired end state that serves as the initial impetus for the planning process. It may also include the commanders' assessment of the adversary commander's intent and an assessment of where and how much risk is acceptable during the operation. [*JP 3-0*]

Composable: A computer system design principle that deals with the inter-relationships of components. A highly composable system provides recombinant components that can be selected and assembled in various combinations to satisfy specific user requirements. The essential attributes that make a component composable are that it be self-contained; that is, modular, and stateless; i.e., treats each request as an independent transaction, unrelated to any previous request.

Defense Support of Civil Authorities: Support provided by U.S. Federal military forces, National Guard forces performing duty in accordance with the Strategy for Homeland Defense and Civil Support, DoD civilians, DoD contract personnel, and DoD component assets, in response to requests for assistance from civil authorities for special events, domestic emergencies, designated law enforcement support, and other domestic activities. Support provided by National Guard forces performing duty in accordance with the Strategy for Homeland Defense and Civil Support is considered DSCA, but is conducted as a State-directed action. Also known as civil support. [DoDD 5111.13, ASD(HD&ASA)]

DoD C2: DoD C2 is a Department-wide C2 capability comprising information integration and decision-support services, systems, processes, and capabilities that enable the exercise of authority and direction over assigned and attached forces, operating in a net-centric, collaborative information environment. [*DoDD O-5100.30*]

Enabler: Any materiel and/or non-materiel "provider" of capability that partially or fully satisfies the operational needs articulated or implied in the DoD C2 Strategic Plan key actions. For example, an *enabler* can be a program, system, development effort, technology, COI, analysis, TTP, doctrine, training initiative, management process or any other effort leading to partial or full satisfaction of key actions.

Enduring Constitutional Government (ECG): A cooperative effort among the Executive, Legislative, and Judicial Branches of the Federal Government, coordinated by the President, to preserve the capability to execute constitutional responsibilities in a catastrophic crisis. ECG is the overarching goal; its objective is the preservation of the constitutional framework under which the Nation is governed. ECG is dependent on effective COOP and COG capabilities.

Interagency: Relating to interaction between agencies, to include federal, state, local and tribal governments.

Interoperability: The ability of systems, units, forces, and mission partners to provide and accept data and services from other systems, units, forces, or mission partners. This also includes the ability to use the data and services to strengthen operational effectiveness, efficiency, and synergy. [*Adapted from JP 1-02 with input from SWarF*.]

Joint Task Force (JTF) Capable Headquarters (HQ): A designated Service HQ that has achieved, and can sustain, a level of readiness to stand up as a JTF HQ, which is acceptable to the supported/assigned combatant commander.

Mission Partners: Those entities not under the commander's direct authority that are participating in the mission. Some examples include, but are not limited to, supported/ supporting commands, non-DoD government agencies such as the Department of State, CIA, or Department of Homeland Security, coalition partners, U.S. and host nation civil authorities, international organizations, and nongovernmental organizations (NGOs).

Net-Centric: Relating to or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data are shared timely and seamlessly among users, applications, and platforms. [Department of Defense Directive 8320.02, December 2, 2004, Data Sharing in a Net-Centric Department of Defense]

Net-Enabled: Not officially defined in DoD. In this document the term is used generically to reflect C2 operations facilitated through the use of information technology (IT) systems interconnected via a communication network or network of networks.

New Triad: In its 2001 Nuclear Posture Review, DOD significantly expanded the range of strategic capabilities to include not only the Old Triad, which consisted of nuclear-armed intercontinental ballistic missiles, submarine-launched ballistic missiles, and strategic bombers, but also conventional and nonkinetic offensive strike and defensive capabilities. The "New Triad" consists of "offensive strike" (the Old Triad), "responsive infrastructure" and "active and passive defenses" along with necessary "command, control, intelligence and planning" capabilities.

Office of Collateral Responsibility (OCR): An organization with responsibilities that relating directly to the subject but without principal responsibility for it. Coordination should occur with the OCR on all significant matters that affect the subject.

Office of Primary Responsibility (OPR): The organization with direct responsibility for the subject.

Rationalization: A systematic method for analyzing the state of systems, applications, and other software within an IT portfolio in order to understand their current condition and cost of operation and support, and to measure their value to current

operations. Typically, this analysis becomes a continuous process, regularly monitoring the state of the portfolio as its IT resources and operational objectives evolve.

Resilient: Capable of recovering quickly from or adjusting to damage, malfunction, or change. Ideally, systems with this attribute are designed to function at their normal operational standard upon recovery. Organizations or systems with few critical failure points and multiple paths have a higher a degree of this attribute than organizations and systems with several critical failure points and one path. [*C2 JIC*]

Responsiveness: Readily reacting to or recovering from changing situations and conditions in real-time and near-real-time. The effective use of responsive and resilient planning, execution, and assessment enables rapid deployment or redirection of assets when various "windows of opportunity" occur. Ideally, systems with this attribute are designed to function at their normal operational standard upon recovery from or reaction to changing situations and conditions. [*C2 JIC*]

Robustness: Full operational functionality due to great strength, durability, survivability, interdependency, resiliency, a distributed nature, or a combination thereof. Organizations and systems with this attribute can function during a disturbance; provide surplus capability to improve service reliability and quality; recover from or adjust to malfunctions or changes; and disperse resources performing services throughout a large area. Organizations and systems with this attribute can operate in several environments and perform effectively across a range of conditions, situations, and missions. Since these systems do not have a single point of failure, any degradation occurs gracefully prior to full system restoration. [*C2 JIC*]

Run-time: In computer science, the duration of a computer program's execution, from beginning to termination. In the current context, it means that if a warfighter generates a short script (program) which utilizes one or more "enterprise service(s)" to accomplish some end, when the script/program executes, the required service functions are accessible and will perform the advertised service. [DoD CIO Memorandum, March 11, 2009, Interim Implementation Guidance for the Net Centric Data Strategy (NCDS) in the Command and Control (C2) Capability Portfolio]

Senior Leaders: Senior leaders are the DoD and national leadership including the President of the United States, Vice President of the United States, the Secretary of Defense, the Deputy Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the combatant commanders, joint task force commanders, joint force component

commanders, and leadership's immediate senior advisors, as appropriate. [*Adapted from DoDD S-5100.44*.]

Senior Warfighter Forum (SWarF): A forum, generally consisting of combatant commands and Services, to organize, analyze, prioritize, and build joint consensus from the warfighter's perspective on complex resource and capabilities needs issues. These forums are delegated by the Chairman of the Joint Chiefs of Staff and are vested in the JROC. [*DoDD 7045.20*]

Service Oriented Architecture (SOA): SOA is an architectural style whose goal is to achieve loose coupling among interacting software agents. A service is a unit of work done by a service provider to achieve desired end results for a service consumer. Both provider and consumer are roles played by software agents on behalf of their owners. SOA is characterized by on-demand services. Participants in a SOA make their resources available by publishing information in structured formats that describe their capabilities and how to access them. Other participants can discover and request those services on demand, but have no power to modify their makeup (other than by feeding back suggestions), ensuring their capabilities always remain available to other participants. This loosely coupled, on-demand assembly of resources has the advantage of being highly adaptable to change.

Service-Oriented Enterprise (SOE): An enterprise that combines a services-focused way of doing business with the latest technology in an operational culture where participating entities are both *service providers* and *service consumers*. This term implies a broader approach to providing and using services than the term service-oriented architecture (SOA), which often implies a particular implementation of a particular architectural or technical construct.

Universal Core (UCore): An interagency information exchange specification and implementation profile. It provides a framework for sharing the most commonly used data concepts of "who, what, when, and where." It serves as a starting point for data level integration and permits the development of richer domain specific exchanges. It was created and is managed by DoD, DOJ, DHS and the Intelligence Community.

Understanding: Having the capacity for rational thought or inference, and the ability to comprehend the meaning and importance of focus areas the commander designates and the direction of his intent. Having the ability to grasp the commander's

guidance and apply it to operations. SA enables situational understanding—knowing what the enemy is doing and why he is doing it. [*C2 JIC*]

ACRONYMS

AMCB	Army-Marine Corps Board
AP	Adaptive Planning
APEX	Adaptive Planning and Execution
AT&L	Acquisition, Technology and Logistics
ATDL	Advanced Tactical Data Link
BA	Battlespace Awareness
BFT	Blue Force Tracker
C2	Command and Control
C2 CIB	C2 Capability Integration Board
C2 CPM	C2 Capability Portfolio Manager
C2ISF	C2 Information Sharing Framework
C&A	Certification & Accreditation
CANES	Consolidated Afloat Networks and Enterprise Systems
CAPE	Cost Assessment and Program Evaluation Office
CAS	Close Air Support
CBA	Capability Based Assessment
CCJO	Capstone Concept for Joint Operations
CDD	Capability Development Document
CDES	Cross Domain Enterprise Service
CDI	Capability Delivery Increment
CID	Combat Identification
CIE	Collaborative Information Environment
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CNCI	Comprehensive National Cybersecurity Initiative
COA	Course of Action
COG	Continuity of Government

COI	Community of Interest
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COP	Common Operational Picture
CPI	Continuous Process Improvement
CPM	Capability Portfolio Manager
CS	Civil Support
C/S/A	Combatant commands/Services/Agencies
DACAS	Digitally Aided Close Air Support
DAS	Defense Acquisition System
DASD	Deputy Assistant Secretary of Defense
DCIN	Defense Continuity Integrated Network
DCO	Defense Collaboration Online
DFCF	Data Flow Configuration File
DIL	Disconnected and Intermittent Connection or Low Bandwidth
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DNLCC	Defense and National Leadership Command Capabilities
DoDD	Department of Defense Directive
DOT&E	Director, Operational Test and Evaluation
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
DSCA	Defense Support of Civil Authorities
DSSC	C2 Capability Portfolio Data and Services Strategy Steering Committee
ECG	Enduring Constitutional Government
ESC	Executive Steering Committee
ESF	Essential Support Function
FCB	Functional Capabilities Board
FFT	Friendly Force Tracking
FITE	Future Immersive Training Environment
FMIP	Force Management Integration Project

FYDP	Future Years Defense Program
GFM	Global Force Management
GFMPEX	GFM Planning and Execution
HD-DSCA	Homeland Defense-Defense Support of Civil Authorities
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICD	Initial Capabilities Document
IFF	Identification Friend or Foe
IOC	Initial Operational Capability
IPL	Integrated Priority List
ISM	Information Security Marking
ISPAN	Integrated Strategic Planning and Analysis Network
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
IW	Irregular Warfare
JAIWG	Joint Architecture Integration Working Group
JCA	Joint Capability Area
JCB	Joint Capability Board
JCCSE	Joint CONUS Communication Support Environment
JCD	Joint Capabilities Document
JCIDS	Joint Capabilities Integration and Development System
JCTD	Joint Capability Technology Demonstration
JCRM	Joint Capabilities Requirements Manager
JFHQ	Joint Force Headquarters
JFS	Joint Fires Support
JIC	Joint Integrating Concepts
JISCC	Joint Incident Site Communications Capability
JOPES	Joint Operation Planning and Execution System
JPME	Joint Professional Military Education
JROC	Joint Requirements Oversight Council

JROCM	JROC Memorandum
JTF	Joint Task Force
JTRS	Joint Tactical Radio System
MCO	Major Combat Operations
MCEITS	Marine Corps Enterprise Information Technology Services
MDR	Metadata Registry
MNIS	Multinational Information Sharing
NC	Net-Centric
NCCS	Nuclear Command and Control System
NCDS	Net-Centric Data Strategy
NCES	Net-Centric Enterprise Services
NC3 LTS	Nuclear Command, Control and Communications – Long Term Solution
NMCS	National Military Command System
NPSUE	National Program for Small Unit Excellence
NS/EP	National Security Emergency Preparedness
NSPD	National Security Presidential Directive
OASD(NII)/ DoD CIO	Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
OCMS	Optimum Capability Mix Study
OCR	Office of Collateral Responsibility
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
PED	Processing, Exploitation, and Dissemination
PMA	Principal Military Advisor
POTUS	President of the United States
PSA	Principal Staff Assistant
PPBE	Planning, Programming, Budgeting, and Execution
QDR	Quadrennial Defense Review
QoS	Quality of Service

SA	Situational Awareness
SLC3S	Senior Leader Command, Control and Communications System
SOA	Service Oriented Architecture
SOE	Service Oriented Enterprise
SSTR	Stability, Security, Transition, and Reconstruction
SWarF	Senior Warfighter Forum
TTP	Tactics, Techniques, and Procedures
UCore	Universal Core
UCP	Unified Command Plan
USD	Under Secretary of Defense
VPOTUS	Vice President of the United States
WIN-T	Warfighter Information Network – Tactical
WMD	Weapons of Mass Destruction